



ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ **Αρ. Φύλλου 87**

26 Ιανουαρίου 2005

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΠΟΦΑΣΕΙΣ

ΑΠΟΦΑΣΕΙΣ

Αριθ. 629 α (1)

Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)

Έχοντας υπόψη:

α. Το Ν. 3115/27.2.2003, άρθρο 1 παραγρ. 1.

β. Το Ν. 3115/27.2.2003, άρθρο 6 παραγρ. 1.

γ. Ότι εκ της παρούσας Αποφάσεως δεν προκύπτει δαπάνη για το Δημόσιο

δ. Τη σχετική εισήγηση της Υπηρεσίας, αποφάσισε:

Κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

Σκοπός του παρόντος Κανονισμού είναι:

1. Η θέσπιση των υποχρεώσεων των φορέων παροχής κινητών τηλεπικοινωνιακών υπηρεσιών για τη διασφάλιση του απορρήτου των κινητών τηλεπικοινωνιακών υπηρεσιών στα πλαίσια της σχετικής Νομοθεσίας Ν. 2225/1994 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/2003 «Περί Διασφάλισης του Απορρήτου των Επικοινωνιών»).

2. Η παρουσίαση βασικών χαρακτηριστικών ασφαλείας των τεχνολογιών κινητών επικοινωνιών δεύτερης και τρίτης γενιάς.

3. Η θέσπιση διαδικασιών ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του παρόντος Κανονισμού υπάγονται όλοι οι τηλεπικοινωνιακοί πάροχοι οι οποίοι παρέχουν Κινητές Τηλεπικοινωνιακές Υπηρεσίες.

Άρθρο 2
Ορισμοί

Για τις ανάγκες του παρόντος Κανονισμού χρησιμοποιούνται οι παρακάτω ορισμοί.

Ακεραιότητα: Η επιβεβαίωση ότι τα δεδομένα τα οποία έχουν σταλεί, έχουν παραληφθεί ή έχουν αποθηκευθεί είναι πλήρη και αμετάβλητα.

Αντίγραφα ασφάλειας: Τα αντίγραφα των ηλεκτρονικών αρχείων πληροφοριών που αφορούν σε δεδομένα επικοινωνίας και χρησιμοποιούνται σε περιπτώσεις καταστροφής των πρωτευόντων αρχείων για την ανάκτησή τους.

Απειλή: Η εν δυνάμει παραβίαση της ασφάλειας ενός συστήματος

Αυθεντικότητα: Η επιβεβαίωση της εγκυρότητας της ταυτότητας.

Δεδομένα θέσης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία στο τηλεπικοινωνιακό δίκτυο και υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας.

Δεδομένα κίνησης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία για να επιτευχθεί η επικοινωνία μέσω του τηλεπικοινωνιακού δικτύου ή για την τιμολόγησή της.

Δημόσιο δίκτυο κινητών επικοινωνιών: Τηλεπικοινωνιακό Δίκτυο αποτελούμενο από τα συστήματα μετάδοσης, τον εξοπλισμό μεταγωγής και τα λοιπά μέσα που επιτρέπουν την μεταφορά σημάτων πληροφορίας με χρήση ραδιοκυμάτων, οπτικών ή άλλων ηλεκτρομαγνητικών μέσων, των οποίων η χρήση είναι εν μέρει ή καθολική για την παροχή διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών σε τερματικά που δεν βρίσκονται σε σταθερές θέσεις.

Δημόσιο τηλεπικοινωνιακό δίκτυο 3ης γενιάς: Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κινητών Επικοινωνιών 3ης Γενιάς (IMT-2000), το οποίο είναι σε θέση να υποστηρίζει καινοτόμες πολυμεσικές υπηρεσίες (πέραν των δυνατο-

τήτων των δικτύων 2ης Γενιάς όπως το GSM) με την υψηλή ταχύτητα επικοινωνίας που εξασφαλίζει μεταξύ τερματικών και δικτύου.

Δημόσιες κινητές τηλεπικοινωνιακές υπηρεσίες: Τηλεπικοινωνιακές υπηρεσίες των οποίων η παροχή συνίσταται, συνολικά ή εν μέρει, στην εγκατάσταση ραδιοεπικοινωνίας με έναν κινητό χρήστη και οι οποίες χρησιμοποιούν, ολικώς ή εν μέρει, ένα Δημόσιο Δίκτυο Κινητών Επικοινωνιών.

Δημόσιες κινητές τηλεπικοινωνιακές υπηρεσίες 2ης γενιάς: οι δημόσιες Τηλεπικοινωνιακές Υπηρεσίες Κινητών Επικοινωνιών που χρησιμοποιούν καθολικά ή εν μέρει ένα Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κινητών Επικοινωνιών 2ης Γενιάς, όπως αυτές οι υπηρεσίες προσδιορίζονται στις Συστάσεις των Τηλεπικοινωνιακών Δικτύων Κινητών Επικοινωνιών όπως το GSM1800 /GSM900.

Δημόσιες κινητές τηλεπικοινωνιακές υπηρεσίες 3ης γενιάς: οι δημόσιες Τηλεπικοινωνιακές Υπηρεσίες Κινητών Επικοινωνιών που χρησιμοποιούν καθολικά ή εν μέρει ένα Δημόσιο Τηλεπικοινωνιακό Δίκτυο Κινητών Επικοινωνιών 3ης Γενιάς, όπως αυτές οι υπηρεσίες προσδιορίζονται στις Συστάσεις των Τηλεπικοινωνιακών Δικτύων Κινητών Επικοινωνιών 3ης Γενιάς, UMTS (IMT-2000) που εκδίδονται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προδιαγραφών (ETSI) και το Διεθνή Οργανισμό Τηλεπικοινωνιών (ITU).

Έλεγχος πρόσβασης: Η πρόληψη μη εξουσιοδοτημένης χρήσης ενός πόρου, συμπεριλαμβανομένης της πρόληψης της χρήσης του πόρου με μη εξουσιοδοτημένο τρόπο.

Εμπιστευτικότητα: Η προστασία των επικοινωνιών ή των αποθηκευμένων δεδομένων από την υποκλοπή και την ανάγνωση από μη εξουσιοδοτημένα άτομα.

Εξουσιοδότηση: Η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητάται η πρόσβαση.

Επίθεση: Οι δραστηριότητες που αναπτύσσονται με σκοπό την παράκαμψη ή την εκμετάλλευση των ατελειών των μηχανισμών ασφάλειας ενός συστήματος. Διακρίνονται σε άμεσες (εκμετάλλευση ατελειών αλγορίθμων, αρχών και ιδιοτήτων του μηχανισμού ασφάλειας) και έμμεσες επιθέσεις (υποχρέωση του συστήματος να χρησιμοποιήσει το μηχανισμό ασφάλειας με λανθασμένο τρόπο, παράκαμψη μηχανισμών).

Επικοινωνία: περιλαμβάνει κάθε είδους επικοινωνία μεταξύ ανθρώπων, αντικειμένων, ανθρώπων και αντικειμένων η οποία γίνεται είτε με τη μορφή του προφορικού ή γραπτού λόγου, είτε με τη μορφή μουσικής, ήχων και εικόνων, είτε με τη μορφή σημάτων είτε και με οποιοδήποτε συνδυασμό όλων αυτών των μορφών.

Κινητό τερματικό: Περιλαμβάνει την κινητή συσκευή και την κάρτα ταυτότητας συνδρομητή (SIM ή USIM) που περιέχει όλα τις πληροφορίες και τα δεδομένα που αφορούν τον συνδρομητή, ενώ η Κινητή Συσκευή ή κινητό τηλέφωνο, μπορεί να είναι κοινή για οποιοδήποτε δίκτυο χρησιμοποιεί ο συνδρομητής.

Προστασία του απορρήτου: Η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα, χωρίς την συγκατάθεσή τους, εξαιρουμένων των περιπτώσεων που προβλέπονται στο σύνταγμα και τους νόμους.

Σταθερές τηλεπικοινωνιακές υπηρεσίες: Οι υπηρεσίες των οποίων η παροχή συνίσταται συνολικά ή εν μέρει στη μετάδοση και δρομολόγηση σημάτων μέσω σταθερών τηλεπικοινωνιακών δικτύων εξαιρουμένων των ραδιοφωνικών και τηλεοπτικών εκπομπών.

Συνδρομητής: Κάθε φυσικό η νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών για την παροχή των υπηρεσιών αυτών.

Σταθμός βάσης: Σταθερός σταθμός του δικτύου κινητών επικοινωνιών που χρησιμοποιείται για την ασύρματη επικοινωνία με τα κινητά τερματικά.

Ταυτότητα: Οι πληροφορίες που προσδιορίζουν το χρήστη με μοναδικό τρόπο.

Τηλεπικοινωνία: Η μεταφορά ήχων, σημάτων, εικόνων, δεδομένων, και εν γένει κάθε φύσης πληροφοριών μεταδιδόμενων εν όλω ή εν μέρει μέσω ενσύρματων, ασύρματων, ηλεκτρομαγνητικών, φωτοηλεκτρονικών ή φωτοοπτικών συστημάτων.

Τηλεπικοινωνιακός πάροχος: Κάθε φυσικό ή νομικό πρόσωπο που παρέχει τηλεπικοινωνιακές υπηρεσίες στο κοινό ή δημόσιο τηλεπικοινωνιακό δίκτυο. Όπου στο κείμενο αναφέρεται ο όρος χωρίς επεξήγηση θα εννοείται ο Πάροχος τηλεπικοινωνιακών υπηρεσιών.

Υπηρεσία κλήσης έκτακτης ανάγκης: Η υπηρεσία λήψης και διαχείρισης κλήσεων έκτακτης ανάγκης που γίνονται προς έναν τηλεφωνικό αριθμό και δρομολογούνται προς ειδικές κρατικές και μη Υπηρεσίες όπως είναι η Αστυνομία, η Πυροσβεστική Υπηρεσία, τα Νοσοκομεία, κ.λπ.

Χρήστης: Κάθε φυσικό πρόσωπο ή νομική οντότητα που χρησιμοποιεί ή ζητά διαθέσιμη στο κοινό τηλεπικοινωνιακή υπηρεσία.

Χρήστης Παρόχου: Κάθε φυσικό πρόσωπο που ανήκει στο προσωπικό ή τους συνεργάτες του Παρόχου και χρησιμοποιεί τα συστήματα και τις υποδομές του Παρόχου.

ΚΕΦΑΛΑΙΟ ΙΙ
Πολιτική Διασφάλισης Απορρήτου Κινητών Τηλεπικοινωνιακών Υπηρεσιών

Άρθρο 3
Ορισμός - Γενικές Απαιτήσεις και Συστάσεις

1. Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΚΤΥ), είναι το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου των επικοινωνιών που διεξάγονται μέσω δικτύων κινητών τηλεπικοινωνιακών επικοινωνιών.

2. Η ΠΔΑΚΤΥ θα εκπονείται από τους τηλεπικοινωνιακούς παρόχους διαθέσιμων στο κοινό κινητών τηλεπικοινωνιακών υπηρεσιών με βάση τις απαιτήσεις και τις υποδείξεις του παρόντος Κανονισμού και θα εφαρμόζεται από αυτούς μετά την έγκρισή της από την ΑΔΑΕ.

3. Η ΠΔΑΚΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική προστασίας των Δικτύων Κινητών Επικοινωνιών, η Πολιτική επεξεργασίας δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το προσωπικό και τους συνεργάτες των τηλεπικοινωνιακών παρόχων, η Πολιτική πρόσβασης, η Πολιτική αποδεκτής χρήσης και η Πολιτική άρσης του απορρήτου από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λει-

τουργία, τη διαχείριση και τη χρήση των τηλεπικοινωνιακών υπηρεσιών.

4. Η ΠΔΑΚΤΥ για να θεωρείται επαρκής θα πρέπει να διαθέτει τουλάχιστον τα ακόλουθα χαρακτηριστικά:

α) Να υλοποιείται μέσω διαδικασιών διαχείρισης συστημάτων, δημοσιοποίησης οδηγιών αποδεκτής χρήσης ή άλλων αντίστοιχων κατάλληλων μεθόδων.

β) Οι διαδικασίες οι οποίες σχετίζονται με την υλοποίηση της πολιτικής πρέπει να περιλαμβάνουν τουλάχιστον τον προσδιορισμό ταυτότητας, την αυθεντικότητα, την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εμπιστευτικότητα, την ακεραιότητα, την προστασία του απορρήτου και τον έλεγχο παραβίασης της ασφάλειας του απορρήτου.

γ) Να εφαρμόζεται μέσω εργαλείων ασφάλειας ή/και μέσω διαδικασιών ασφάλειας.

δ) Να καθορίζει τις περιοχές ευθύνης των χρηστών και των χρηστών παρόχου. Επιπλέον οι μηχανισμοί μεταβολής της πολιτικής διασφάλισης του απορρήτου πρέπει να είναι καλά ορισμένοι, περιλαμβάνοντας τη διαδικασία, τους εμπλεκόμενους, καθώς και τους υπεύθυνους προς έγκριση.

5. Επίσης, συνιστάται η ΠΔΑΚΤΥ:

α) Να είναι ανεξάρτητη, στο μέτρο που είναι δυνατόν από τεχνικής απόψεως, από συγκεκριμένο εξοπλισμό (υλικό, λογισμικό) και

β) Να βασίζεται σε μια ανοικτή αρχιτεκτονική έτσι ώστε να καθίσταται βιώσιμη μακροπρόθεσμα.

6. Η ΠΔΑΚΤΥ υπόκειται σε έλεγχο από την ΑΔΑΕ, τόσο ως προς την πληρότητα και αποτελεσματικότητά της, όσο και ως προς τον βαθμό εφαρμογής της.

Άρθρο 4
Χάραξη και στοιχεία Πολιτικής Διασφάλισης Απορρήτου Κινητών Τηλεπικοινωνιακών Υπηρεσιών

1. Ένας τηλεπικοινωνιακός πάροχος προκειμένου να χαράξει την πολιτική του μπορεί, χωρίς να υποχρεώνεται ή να περιορίζεται, να ακολουθήσει τα παρακάτω βήματα:

α) Να προσδιορίσει τις πληροφορίες που πρέπει να προστατευτούν.

β) Να προσδιορίσει τα ευάλωτα σημεία του τηλεπικοινωνιακού δικτύου.

γ) Να προσδιορίσει τους κινδύνους και τις απειλές για τα α), β).

δ) Να προσδιορίσει τα μέτρα διασφάλισης της προστασίας του απορρήτου στις κινητές Τηλεπικοινωνιακές Υπηρεσίες.

ε) Να καθορίσει τις υποχρεώσεις των υπαλλήλων και συνεργατών του.

στ) Να καθορίσει τις δεσμεύσεις και υποχρεώσεις του έναντι των πελατών του.

ζ) Να καταρτίσει σχέδιο αναθεώρησης και βελτίωσης της ΠΔΑΚΤΥ κάθε φορά που θα εντοπίζεται νέος κίνδυνος ή αδυναμία ή που θα προκύπτουν νέες τεχνολογικές διευκολύνσεις διαχείρισης ασφάλειας.

2. Κάθε τηλεπικοινωνιακός πάροχος πρέπει, και σε περίπτωση που απαιτείται σε συνεργασία με τους παρόχους τηλεπικοινωνιακού δικτύου, να τεκμηριώνει με σχέδια την προστασία του απορρήτου για να αντιμετωπίσει προβλήματα που πιθανώς να εμφανισθούν σε έκτακτες περιστάσεις, όπως είναι η άρση του απορρήτου μετά από εντολή δικαστικών ή εισαγγελικών αρχών (Νόμος 2225) και η προβληματική λειτουργία των τηλεπικοινωνιακών ή/και των μηχανογραφικών συστημάτων του ή των συστημάτων των συνεργατών του.

Άρθρο 5
Προστατευόμενα στοιχεία κινητών επικοινωνιών

1. Κάθε πάροχος κινητών τηλεπικοινωνιακών υπηρεσιών οφείλει να διασφαλίζει και να προστατεύει το απόρρητο των διαφόρων δεδομένων Επικοινωνίας του περιεχόμενου της επικοινωνίας, και εν γένει κάθε πληροφορίας που αφορά τους συνδρομητές του και χρησιμοποιείται για την παροχή της τηλεπικοινωνιακής υπηρεσίας, τη διεκπεραίωση της επικοινωνίας, κ.τ.λ.

2. Σε συγκεκριμένο φυσικό ή νομικό πρόσωπο, που είναι συνδρομητής ή χρήστης ενός παρόχου κινητών τηλεπικοινωνιακών υπηρεσιών πρέπει να προστατεύεται το απόρρητο των ακόλουθων στοιχείων εισερχομένων και εξερχομένων κλήσεων:

α) Καλών και καλούμενος αριθμός,

β) Καλών και καλούμενος συνδρομητής-χρήστης,

γ) Χρόνος και διάρκεια επικοινωνίας,

δ) Εντοπισμός καλούντος ή και καλούμενου χρήστη,

ε) Στοιχεία που αφορούν στη χρέωση της επικοινωνίας,

στ) Περιεχόμενο και δεδομένα επικοινωνίας,

ζ) Ταυτότητα κινητής τερματικής συσκευής και ταυτότητα σύνδεσης.

3. Οι πάροχοι κινητών τηλεπικοινωνιακών υπηρεσιών θα πρέπει να προσδιορίζουν τους κινδύνους και τις ενδεχόμενες απειλές για τα παραπάνω στοιχεία. Ο πάροχος οφείλει να διασφαλίζει το απόρρητο της μετάδοσης και αποθήκευσης των δεδομένων Επικοινωνίας που χρησιμοποιούνται σε ένα δίκτυο κινητών επικοινωνιών. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να ενημερώνει τους συνδρομητές του με συγκεκριμένους τρόπους και μέσα της επιλογής του για οποιουσδήποτε ειδικούς κινδύνους σχετικά με την ασφάλεια των υπηρεσιών που παρέχει καθώς επίσης και οποιωνδήποτε δυνατοτήτων για την απομάκρυνση των κινδύνων και του κόστους των μέτρων που περιλαμβάνονται.

Άρθρο 6
Ευάλωτα Σημεία Δικτύου Κινητών Επικοινωνιών

Ενδεικτικά αναφέρονται ευάλωτα σημεία σε επιθέσεις και παραβιάσεις:

1. Τερματικών συσκευών χρηστών:

α) Η ίδια η συσκευή

β) Το αρχείο των εξερχόμενων ή εισερχόμενων κλήσεων

γ) Το αρχείο των καλούντων και καλούμενων αριθμών

δ) Ο τυχόν ενσωματωμένος αυτόματος τηλεφωνητής

ε) Τυχόν μνήμη καταγραφής

στ) Κάρτα Ταυτότητας Συνδρομητή (SIM)

2. Δικτύου:

α) Σταθμός Βάσης

β) Μικροκυματικές Ραδιοζεύξεις (μεταξύ σταθμών βάσης, κ.α.)

γ) Αλγόριθμοι Κρυπτογράφησης

δ) Διακομιστές (servers)

ε) Το φωνητικό ταχυδρομείο (Voice mail).

στ) Κεντρικοί κατανεμητές Παρόχου

ζ) Κέντρα μεταγωγής και συνδέσεις του δικτύου κινητών επικοινωνιών με το σταθερό τηλεπικοινωνιακό δίκτυο

η) Οι δρομολογητές κλήσεων όταν υπάρχει εκτροπή των κλήσεων σε εναλλακτικό φορέα παροχής τηλεπικοινωνιακών υπηρεσιών

θ) Η αποκάλυψη κλειδιών που χρησιμοποιούνται για κρυπτογράφηση.

Ο πάροχος κινητών τηλεπικοινωνιακών υπηρεσιών θα πρέπει να ενημερώνει τους χρήστες με συγκεκριμένα μέ-

σα (γραπτές οδηγίες κ.λπ.) για τα ευάλωτα σημεία που ανήκουν στην περιοχή ευθύνης τους και θα λαμβάνει όλα τα προσήκοντα μέτρα για την προστασία των ευάλωτων σημείων που ανήκουν στην δικαιοδοσία του.

ΚΕΦΑΛΑΙΟ ΙΙΙ
Επιμέρους Πολιτικές Διασφάλισης Απορρήτου Κινητών Τηλεπικοινωνιακών Υπηρεσιών

Άρθρο 7
Ασφάλεια Δικτύων Κινητών Επικοινωνιών Δεύτερης Γενιάς

1. Η ασφάλεια ενός δικτύου κινητών επικοινωνιών δεύτερης γενιάς θα πρέπει να καλύπτει τις απαιτήσεις τόσο του παρόχου όσο και του συνδρομητή.

2. Ένας τηλεπικοινωνιακός πάροχος, διαχειριστής ενός δικτύου κινητών επικοινωνιών 2ης γενιάς, πρέπει να χρησιμοποιεί τις προτεινόμενες διαδικασίες ασφαλείας σχετικές με: α) την δημιουργία και διανομή των κλειδιών, β) την ανταλλαγή πληροφοριών με άλλους διαχειριστές και γ) το απόρρητο των αλγορίθμων.

3. Οι βασικοί στόχοι ασφάλειας για ένα πάροχο κινητών τηλεπικοινωνιακών υπηρεσιών μέσων ενός δικτύου κινητών επικοινωνιών 2ης γενιάς είναι:

α) Το απόρρητο της ταυτότητας του συνδρομητή, ώστε να μην μπορεί κάποιος τρίτος να γνωρίζει πότε και από που χρησιμοποιεί ο συνδρομητής το δίκτυο. Για να επιτευχθεί το απόρρητο της ταυτότητας του συνδρομητή, του αποδίδονται προσωρινές ταυτότητες. Κάθε συνδρομητής έχει μία Διεθνή Ταυτότητα Συνδρομητή η οποία είναι παγκοσμίως μοναδική και είναι αποθηκευμένη στην κάρτα SIM (Subscriber Identity Module). Η Διεθνής Ταυτότητα Συνδρομητή χρησιμοποιείται μόνο όταν δεν υπάρχει άλλος τρόπος να αναγνωρισθεί ο Συνδρομητής. Αυτό μπορεί να συμβεί κατά την διαδικασία δημιουργία της πρώτης σύνδεσης ενός καινούριου Συνδρομητή ή εφόσον υπάρξει κάποια απώλεια δεδομένων στο δίκτυο. Επιπλέον, στην διάρκεια της σύνδεσης στο δίκτυο, δίνεται σε τακτά χρονικά διαστήματα καινούρια Προσωρινή Ταυτότητα στον Κινητό Σταθμό, κάτι που καθιστά αρκετά δύσκολη την προσπάθεια γεωγραφικού εντοπισμού του Συνδρομητή. Εφόσον δεν υπάρχει κάποιο πρόβλημα με το δίκτυο, με κανένα τρόπο δεν πρέπει να μεταδίδεται η Διεθνής Ταυτότητα μέσω του αέρα σε καμιά άλλη περίπτωση εκτός από την διαδικασία της αρχικής σύνδεσης.

β) Η πιστοποίηση της ταυτότητας του συνδρομητή, ώστε ο διαχειριστής να είναι σίγουρος ότι χρεώνει το σωστό άτομο. Η διαδικασία πιστοποίησης στις κινητές επικοινωνίες 2ης γενιάς είναι μια μονομερής διαδικασία αφού ο Συνδρομητής δεν μπορεί να πιστοποιήσει την ταυτότητα του δικτύου. Βασικό ρόλο στη διαδικασία πιστοποίησης διαδραματίζει ο Αλγόριθμος Πιστοποίησης Α3, ο οποίος δεν είναι απαραίτητα κοινός για όλα τα δίκτυα αλλά για να υπάρχει συμβατότητα μεταξύ τους, οι βασικές του παράμετροι καθορίζονται από την κοινοπραξία GSM.

γ) Η προστασία των δεδομένων σηματοδοσίας, ώστε δεδομένα όπως αριθμοί τηλεφώνου να μην μπορούν να υποκλαπούν.

δ) Η προστασία της συνομιλίας, ώστε να προστατευτεί το απόρρητο της συνομιλίας. Η προστασία των δεδομένων Επικοινωνίας είναι επίσης απαραίτητη.Η χρησιμοποίηση ή μη της κρυπτογράφησης εξαρτάται από το δίκτυο κινητών επικοινωνιών και όχι από τον συνδρομητή. Μόνο ο σταθμός βάσης μπορεί να στείλει εντολή στον κινητό τερματικό σταθμό ώστε να ξεκινήσει η κρυπτογράφηση και από τις δύο πλευρές. Οι αλγόριθμοι, που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων, είναι γνωστοί ως Α8 και Α5 και είναι αποθηκευμένοι, ο μεν πρώτος στην κάρτα SIM και ο δεύτερος στην κινητή συσκευή. Συνήθως ο αλγόριθμος Α8 συνδυάζεται μαζί με το Α3 σε ένα νέο αλγόριθμο, τον Α3/8. Εφόσον υπάρχουν διαφορετικές εκδόσεις του αλγόριθμου Α5, πριν αρχίσει η κρυπτογράφηση είναι απαραίτητο να ενημερωθεί ο Σταθμός Βάσης για την έκδοση του αλγορίθμου που χρησιμοποιεί ο Κινητός Σταθμός. Το κλειδί κρυπτογράφησης πρέπει να ανανεώνεται κάθε φορά που πιστοποιείται η ταυτότητα του Συνδρομητή από το Δίκτυο και αυτό πρέπει να γίνεται πριν από κάθε κλήση ή κάθε φορά που ο Συνδρομητής επιθυμεί να συνδεθεί στο δίκτυο εκ νέου. Η συχνότητα της πιστοποίησης από τον Διαχειριστή του Δικτύου Κινητών Επικοινωνιών πρέπει να είναι τέτοια ώστε να ελαχιστοποιούνται οι πιθανότητες υποκλοπής δεδομένων συνομιλίας και σηματοδοσίας.

4. Περιπτώσεις απειλών του συστήματος ασφαλείας ενός δικτύου κινητών επικοινωνιών δεύτερης γενιάς:

α) Απόκτηση πρόσβασης στο δίκτυο κορμού
β) Επιθέσεις στην κάρτα SIM
γ) Επίθεση στο αλγόριθμο Α5
δ) Επίθεση με απομίμηση σταθμού βάσης
ε) Άρνηση των υπηρεσιών για ένα συνδρομητή λόγω παρεμβολής.

Άρθρο 8
Ασφάλεια Δικτύων Κινητών Επικοινωνιών Τρίτης Γενιάς

1. Η ασφάλεια ενός δικτύου κινητών επικοινωνιών τρίτης γενιάς περιλαμβάνει τις παρακάτω βασικές αρχές:

α) Τα δεδομένα που σχετίζονται ή δημιουργούνται από τον χρήστη είναι επαρκώς προστατευμένα από κακή χρήση ή κατάχρηση

β) Οι υπηρεσίες που παρέχονται από τα δίκτυα εξυπηρέτησης και τους καταχωρητές στους σταθμούς βάσης είναι επαρκώς προστατευμένες από κακή χρήση ή κατάχρηση.

γ) Οι διαδικασίες ασφαλείας πρέπει να είναι επαρκώς ορισμένες ώστε να διασφαλιστεί η παγκόσμια χρήση τους και η περιαγωγή μεταξύ διαφορετικών δικτύων εξυπηρέτησης.

δ) Οι διαδικασίες και οι μηχανισμοί ασφαλείας πρέπει να μπορούν να επεκταθούν ή να αναθεωρηθούν ανάλογα με τις καινούριες απαιτήσεις που θα προκύψουν στο μέλλον.

2. Ένα δίκτυο κινητών επικοινωνιών τρίτης γενιάς πρέπει να χαρακτηρίζεται από όλες τις τεχνικές ασφαλείας που προστέθηκαν σε σχέση με τα δίκτυα κινητών επικοινωνιών δεύτερης γενιάς δηλαδή: πιστοποίηση της ταυτότητας του δικτύου και από τον συνδρομητή ώστε να αποκλείονται έτσι τις επιθέσεις «ψεύτικου σταθμού βάσης», αύξηση του μήκους των κλειδιών πιστοποίησης και κρυπτογράφησης με αποτέλεσμα τη δημιουργία ισχυρότερων αλγόριθμων, εισαγωγή μηχανισμών ασφαλείας τόσο μέσα στο δίκτυο όσο και μεταξύ των δικτύων και τέλος, προστασία των διασυνδέσεων μεταξύ Σταθμού Βάσης και Ελεγκτή. Σε ένα δίκτυο κινητών επικοινωνιών τρίτης γενιάς οι διαδικασίες ασφαλείας πρέπει να αντιμετωπίζονται με ενιαίο τρόπο.

3. Περιπτώσεις απειλών του συστήματος ασφαλείας ενός δικτύου κινητών επικοινωνιών τρίτης γενιάς:

α) Επιθέσεις στην κάρτα USIM
β) Επίθεση στο αλγόριθμο f8
γ) Επίθεση στο αλγόριθμο f9
δ) Επίθεση στην σηματοδοσία και στην διαδικασία επανασυγχρονισμού

ε) Επίθεση στις διαδικασίες που χρησιμοποιούνται για την πιστοποίηση και τη διευθέτησης κλειδιών

ζ) Επίθεση στους διαδοχικούς αριθμούς (SQN) οι οποίοι εξασφαλίζουν στο συνδρομητή ότι τα δεδομένα πιστοποίησης δεν έχουν ξαναχρησιμοποιηθεί.

4. Σε ένα δίκτυο κινητών επικοινωνιών με μικτά τμήματα δεύτερης και τρίτης γενιάς, θα εφαρμοστεί η διαδικασία Πιστοποίησης και Διευθέτησης Κλειδιών δεύτερης γενιάς αν ένα τουλάχιστον τμήμα, εξαιρουμένου του Υποσυστήματος Σταθμού Βάσης, είναι δεύτερης γενιάς. Αντίθετα για να πραγματοποιηθεί η διαδικασία Πιστοποίησης και Διευθέτησης Κλειδιών τρίτης γενιάς θα πρέπει όλα τα τμήματα, εξαιρουμένου του Υποσυστήματος Σταθμού Βάσης, να είναι τρίτης γενιάς.

5. Οι πάροχοι κινητών τηλεπικοινωνιακών υπηρεσιών 3ης γενιάς υποχρεούνται να ενημερώνουν τους συνδρομητές τους για την αλληλεπίδραση μεταξύ καρτών SIM, USIM και κινητών συσκευών με αποτέλεσμα την ενδεχόμενη έλλειψη ασφαλείας στις επικοινωνίες τους.

Άρθρο 9
Προστασία δικτύων κινητών επικοινωνιών

1. Η ασφάλεια δικτύων επικοινωνίας περιλαμβάνει: α) τις απειλές που οφείλονται στην εμπεριεχόμενη αξιοπιστία του ίδιου του δικτύου κινητών επικοινωνιών, και β) την ευαισθησία του στις απειλές από κακόβουλες πράξεις. Η ΑΔΑΕ αναγνωρίζει ότι η πηγή απειλής μπορεί να προέλθει από ένα άλλο διασυνδεόμενο δίκτυο τηλεπικοινωνιών (σταθερό, ασύρματο) και αυτό είναι εφικτό για το λόγο ότι η σηματοδοσία στο σταθερό τηλεφωνικό δίκτυο δεν είναι κρυπτογραφημένη. Για αυτό το λόγο η πολιτική ασφάλειας των παρόχων πρέπει να επιδιώκει να εντοπίζει τα σημεία που πρέπει να δοθεί ιδιαίτερη προσοχή.

2. Απαιτείται να λαμβάνονται τα απαραίτητα μέτρα για τη σωστή χωροθέτηση του τηλεπικοινωνιακού εξοπλισμού του παρόχου, την προστασία των γραμμών μεταφοράς του δικτύου καθώς και όλων των στοιχείων του δικτύου, συμπεριλαμβανομένων των ιστών των κεραιών, ώστε να εξασφαλίζονται έναντι κακοβούλων επιθέσεων και έναντι άλλων μορφών φυσικών παρεμβάσεων.

3.Τα σημεία εισόδου από άλλα τηλεπικοινωνιακά δίκτυα πρέπει να ελέγχονται επισταμένως.

4. Πρέπει να λαμβάνονται όλα τα απαραίτητα μέτρα προστασίας για τα ευάλωτα σημεία του δικτύου που αναφέρονται στο άρθρο 7 του παρόντος.

Άρθρο 10
Προστασία επεξεργασίας των δεδομένων Επικοινωνίας

Οι πάροχοι κινητών τηλεπικοινωνιακών υπηρεσιών οφείλουν να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της κείμενης νομοθεσίας για την προστασία της επεξεργασίας των δεδομένων Επικοινωνίας.

Άρθρο 11
Ασφάλεια σε σχέση με τους Χρήστες Παρόχου

Οι χρήστες παρόχου οφείλουν να συμμορφώνονται με τις διατάξεις της νομοθεσίας περί προστασίας του απορρήτου.

Ειδικότερα:

α) Απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που συνδέονται με: i) το περιεχόμενο ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω παρόχου υπηρεσιών επικοινωνιών ή ii) υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο μέσω ενός παρόχου υπηρεσιών επικοινωνιών ή iii) τα δεδομένα Επικοινωνίας που υποπίπτουν στην αντίληψη ή στην κατοχή του ως αποτέλεσμα της φύσης της εργασίας του.

γ) Όσοι διαχειρίζονται ή έχουν πρόσβαση στη βάση δεδομένων των συνδρομητών απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που συνδέονται με: i) υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο μέσω ενός παρόχου υπηρεσιών επικοινωνιών ή ii) τα δεδομένα Επικοινωνίας που υποπίπτουν στην αντίληψη ή στην κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

δ) Οι χρήστες παρόχου που διαχειρίζονται κλήσεις έκτακτης ανάγκης απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία συνδέονται με: i) το περιεχόμενο ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω του τηλεπικοινωνιακού παρόχου ή ii) τα δεδομένα Επικοινωνίας (όπως μη ανακοινώσιμες συνδέσεις και διευθύνσεις) που υποπίπτουν στην αντίληψη ή στην κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

Οι εξαιρέσεις των προηγούμενων γενικών κανόνων, που επιβάλλονται για λόγους λειτουργίας του παρόχου ή προβλέπονται στην ισχύουσα νομοθεσία, θα περιγράφονται με σαφήνεια στην πολιτική ασφάλειας του τηλεπικοινωνιακού παρόχου.

Άρθρο 12
Πολιτική πρόσβασης

1. Η Πολιτική Πρόσβασης καθορίζει το επίπεδο πρόσβασης χρηστών παρόχου και διεργασιών λογισμικού σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου για την παροχή των κινητών τηλεπικοινωνιακών υπηρεσιών.

2. Η Πολιτική Πρόσβασης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΚΤΥ.

3. Ο πάροχος οφείλει να διαθέτει και να εφαρμόζει Πολιτική Πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες φωνής και δεδομένων, τηλεπικοινωνιακές συσκευές και προγράμματα λογισμικού.

4. Η Πολιτική Πρόσβασης περιγράφει για κάθε σύστημα, με τρόπο λεπτομερή και σαφή, τουλάχιστον τις ακόλουθες διαδικασίες:

(α) Διαδικασίες προσθήκης νέων χρηστών και χρηστών παρόχου στο συγκεκριμένο δίκτυο κινητών επικοινωνιών

(β) Διαδικασίες εξουσιοδότησης σχετικά με την προσθήκη, διαγραφή και αλλαγή των επιπέδων πρόσβασης των χρηστών παρόχου σε τηλεπικοινωνιακές υπηρεσίες του εν λόγω συστήματος.

(γ) Διαδικασίες ταυτοποίησης χρηστών

(δ) Τρόπους ελέγχου των παραπάνω διαδικασιών και διαχείρισης του επιπέδου πρόσβασης που παραχωρείται στους χρήστες παρόχου

(ε) Διαδικασίες πρόσβασης των χρηστών παρόχου των κινητών τηλεπικοινωνιακών υπηρεσιών σε συστήματα που διατηρούν δεδομένα κίνησης και θέσης χρηστών

(στ) Σε περίπτωση που χρησιμοποιείται κρυπτογράφηση, η Πολιτική Πρόσβασης θα πρέπει να περιέχει τις διαδικασίες πρόσβασης των χρηστών παρόχου σε συστήματα κρυπτογράφησης/αποκρυπτογράφησης καθώς και σε διαδικασίες σχετικά με την διαχείριση, διανομή, εισαγωγή και αρχειοθέτηση των κλειδιών κρυπτογράφησης. Οι πληροφορίες αυτές θα αναφέρονται σε καταλλήλως διαβαθμισμένο παράρτημα των εγγράφων που περιέχουν την Πολιτική Πρόσβασης.

Άρθρο 13
Πολιτική Αποδεκτής Χρήσης

1. Η Πολιτική Αποδεκτής Χρήσης περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών και χρηστών παρόχου των συστημάτων μετάδοσης του δικτύου κινητών επικοινωνιών ενός παρόχου.

2. Η Πολιτική Αποδεκτής Χρήσης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΚΤΥ.

3. Σκοπός της είναι να διασφαλίσει ότι οι χρήστες και οι χρήστες παρόχου δεν θα εκμεταλλευτούν την πρόσβαση που τους παρέχεται σύμφωνα με την Πολιτική Πρόσβασης σε παντός είδους τηλεπικοινωνιακά δίκτυα προκειμένου να προβούν σε ενέργειες που παραβιάζουν οποιονδήποτε νόμο του κράτους.

4. Η Πολιτική Αποδεκτής Χρήσης πρέπει να είναι προσαρμοσμένη στην κατηγορία χρηστών στην οποία απευθύνεται (χρηστών και χρηστών παρόχου) και να είναι σύμφωνη με την Πολιτική Πρόσβασης για κάθε κατηγορία χρηστών.

5. Η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει, με όσο το δυνατόν πιο λεπτομερή και κατανοητό τρόπο ώστε να αποφεύγονται οι παρερμηνείες, το ακόλουθο ελάχιστο περιεχόμενο:

(α) Δικαιώματα χρήστη και χρήστη παρόχου. Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης.

(β) Υποχρεώσεις χρήστη και χρήστη παρόχου. Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα μη αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης, καθώς και συνέπειες μη συμμόρφωσης με αυτές τις υποχρεώσεις.

(γ) Δικαιώματα του παρόχου κινητών τηλεπικοινωνιακών υπηρεσιών.

(δ) Υποχρεώσεις του τηλεπικοινωνιακού παρόχου κινητών υπηρεσιών.

6. Επιπλέον στην ενότητα που αναφέρεται στις υποχρεώσεις των χρηστών, η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει τις παρακάτω διατάξεις οι οποίες σχετίζονται με την ασφάλεια του συστήματος:

(α) Οι χρήστες οφείλουν να λαμβάνουν όλα τα ενδεικνυόμενα μέτρα για την διασφάλιση του απορρήτου επικοινωνιών τους.

(β) Οι χρήστες οφείλουν να ενημερώνουν αμέσως τους υπευθύνους του παρόχου αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών.

(γ) Οι χρήστες οφείλουν να αποκτούν πρόσβαση αποκλειστικά και μόνο σε δεδομένα κίνησης ή θέσης τα οποία αναφέρονται στους ίδιους ή είναι Δημοσίως Ανακοινώσιμα κατά την Πολιτική Ευαισθησίας Πληροφοριών ή για τα οποία τους έχει δοθεί πρόσβαση κατά την Πολιτική Πρόσβασης.

(δ) Οι χρήστες απαγορεύεται να επιχειρούν να εκμεταλλευτούν πιθανά κενά ασφάλειας των συστημάτων του παρόχου προκειμένου να αποκτήσουν πρόσβαση σε πληροφορίες άλλων χρηστών, να διαταράξουν την ομαλή λειτουργία των δικτύων, να εκτελέσουν κακόβουλο λογισμικό και γενικά να υποβαθμίσουν το επίπεδο ασφάλειας του συστήματος.

7. Ο πάροχος οφείλει να δίνει στο χρήστη πρόσβαση στα συστήματά του μόνο εφόσον ο χρήστης έχει λάβει γνώση και ακολούθως έχει αποδεχθεί την Πολιτική Αποδεκτής Χρήσης. Το γεγονός αυτό αποδεικνύεται είτε με έγγραφη δήλωση του χρήστη η οποία φέρει την πρωτότυπη υπογραφή του ή εφόσον ο χρήστης έχει συμπληρώσει το αντίστοιχο πεδίο σε σχετική φόρμα αποδοχής στην περίπτωση που η Πολιτική Αποδεκτής Χρήσης παρουσιάζεται ηλεκτρονικά.

ΚΕΦΑΛΑΙΟ IV
Υποχρεώσεις φορέων, Έλεγχος και Εποπτεία

Άρθρο 14
Υποχρεώσεις φορέων αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών

1. Όλοι οι τηλεπικοινωνιακοί πάροχοι υποχρεούνται:

(α) Να διαθέτουν ανά πάσα στιγμή καθορισμένη πολιτική για τη διασφάλιση του απορρήτου τηλεπικοινωνιακών υπηρεσιών παρεχομένων από δημόσια τηλεπικοινωνιακά δίκτυα κινητών επικοινωνιών.

(β) Να εφαρμόζουν την εν λόγω πολιτική.

(γ) Να ενημερώσουν σχετικά ως προς την εφαρμοζόμενη πολιτική την ΑΔΑΕ εντός έξι μηνών από την δημοσίευση του παρόντος.

(δ) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική εντός ενός έτους από την έγκρισή της.

2. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβλέπει στο οργανόγραμμά του ξεχωριστή διοικητική οντότητα η οποία θα είναι επιφορτισμένη με την κατάρτιση και την εφαρμογή της ΠΔΑΚΤΥ με επικεφαλής κατάλληλα καταρτισμένο στέλεχός του που θα φέρει τον τίτλο του Υπευθύνου Ασφαλείας.

3. Για την αποτελεσματική εφαρμογή της Πολιτικής Πρόσβασης ο κάθε τηλεπικοινωνιακός πάροχος οφείλει να ορίζει τουλάχιστον:

(α) Έναν Υπεύθυνο Πρόσβασης, ο οποίος θα καθορίζει το είδος της πρόσβασης των χρηστών στα συστήματα.

(β) Έναν Υπεύθυνο Συστήματος, ο οποίος θα υλοποιεί τις αποφάσεις του Υπευθύνου Πρόσβασης.

(γ) Έναν Υπεύθυνο Αντιγράφων Ασφαλείας, ο οποίος πάντα σε συνεννόηση με τον Υπεύθυνο Πρόσβασης θα καθορίζει ποιος έχει πρόσβαση στα αντίγραφα ασφαλείας καθώς και το χρονικό διάστημα λήψης τους.

4. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβαίνει σε τακτικές επισκοπήσεις και αναθεωρήσεις της πολιτικής διασφάλισης του απορρήτου, είτε αυτόβουλα (μετά από έγκριση της ΑΔΑΕ σε περίπτωση αναθεώρησης) είτε ύστερα από σχετική εντολή της ΑΔΑΕ όπως μπορεί να προκύψει από πιθανή διαδικασία ελέγχου ή έκδοση σχετικής οδηγίας.

5. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου ο πάροχος οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους) και να παρέχει στοιχεία για την αποτροπή ή αντιμετώπισή τους.

6. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου που δεν είναι δυνατό να αντιμετωπιστεί με τα τρέχοντα μέσα που διαθέτει ο τηλεπικοινωνιακός πάροχος, αυτός οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπει-

ες αυτών (συμπεριλαμβανομένου του πιθανού κόστους).

7. Ο πάροχος οφείλει να ενημερώνει τους χρήστες για την ύπαρξη και τον τρόπο χρήσης τεχνολογιών-πόρων σχετικών με την ασφάλεια των μεταδιδομένων πληροφοριών.

8. Ο πάροχος οφείλει να ορίζει συνέπειες για τη μη συμμόρφωση των χρηστών παρόχου με τα προβλεπόμενα από την ΠΔΑΚΤΥ του Απορρήτου (συμπεριλαμβανομένων των Πολιτικών Πρόσβασης και Αποδεκτής χρήσης).

Άρθρο 15
Διαδικασία Έλεγχου από την ΑΔΑΕ - Κυρώσεις

1. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του παρόντος. Η συχνότητα των ελέγχων θα καθοριστεί από την ΑΔΑΕ με μεταγενέστερη Απόφαση της.

2. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες υπηρεσίες της ΑΔΑΕ ή από ειδικούς που τελούν υπό την άμεση επίβλεψη της ΑΔΑΕ, με την παρουσία εξουσιοδοτημένου προσώπου του παρόχου, σύμφωνα με τη διαδικασία που περιγράφεται στο Παράρτημα Α του παρόντος Κανονισμού.

3. Κατά την διάρκεια του ελέγχου η ΑΔΑΕ καταγράφει αναλυτικά τις ενέργειες σε ειδικό έντυπο με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Πάροχο Κινητών Τηλεπικοινωνιακών Υπηρεσιών αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών». Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β του παρόντος Κανονισμού.

4. Η ομάδα ελέγχου κοινοποιεί το πόρισμά της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου λαμβάνοντας υπόψη και τις πιθανές ενστάσεις του παρόχου και είτε εγκρίνει τις ενέργειες που προβλέπονται στην εκάστοτε πολιτική προστασίας του απορρήτου του παρόχου που έχει εγκριθεί από την ΑΔΑΕ είτε επιβάλλει κυρώσεις εφόσον κρίνει ότι δεν έχουν ληφθεί τα προσήκοντα μέτρα, με βάση τα αναφερόμενα στην εγκεκριμένη ΠΔΑΚΤΥ.

5. Η ΑΔΑΕ διενεργεί έκτακτους ελέγχους σε περίπτωση δημόσιων καταγγελιών ή έγγραφων καταγγελιών εκ μέρους των χρηστών. Εφόσον πρόκειται για δημόσιες καταγγελίες, ακολουθείται η διαδικασία που προβλέπεται για τους τακτικούς ελέγχους, ενώ στην περίπτωση εμπιστευτικών έγγραφων καταγγελιών εκ μέρους χρηστών, ο έλεγχος μπορεί κατά την κρίση της ΑΔΑΕ να γίνει αιφνιδιαστικά.

6. Ως προς τη διαδικασία και τις κυρώσεις της παραγράφου 5, ισχύουν οι διατάξεις του Νόμου 3115, άρθρο 11 και άρθρο 6, παράγραφος 4, καθώς και τα προβλεπόμενα στον εσωτερικό κανονισμό της ΑΔΑΕ (ΦΕΚ 1642/Β/7.11.2003).

Άρθρο 16
Άσκηση Εποπτείας

Κάθε πάροχος κινητών τηλεπικοινωνιακών υπηρεσιών στο τέλος του ημερολογιακού έτους υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν στην ασφάλεια των κινητών επικοινωνιών και τη διασφάλιση του απορρήτου.

Το ελάχιστο περιεχόμενο της ετήσιας έκθεσης ορίζεται ως εξής:

(α) Περιστατικά που απείλησαν την ασφάλεια του παρόχου και τη διασφάλιση του απορρήτου καθώς και τυχόν βλάβες που υπέστη ο πάροχος και οι χρήστες του εξαιτίας αυτών.

(β) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της ετήσιας έκθεσης.

Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τους φορείς οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στα πλαίσια των αρμοδιοτήτων της για την ασφάλεια των κινητών επικοινωνιών και τη διασφάλιση του απορρήτου.

Άρθρο 17
Προστασία Επεξεργασίας Αρχείων

Σε περιπτώσεις παραβίασης των διατάξεων προστασίας του απορρήτου των επικοινωνιών, οι οποίες περιλαμβάνουν και επεξεργασία αρχείων που αφορούν την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η ΑΔΑΕ θα την ενημερώνει σχετικά προκειμένου να επιλαμβάνεται στο πλαίσιο των δικών της αρμοδιοτήτων.

ΚΕΦΑΛΑΙΟ V
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 18
Έναρξη Ισχύος

1.Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α
Αναλυτική περιγραφή διαδικασίας
Ελέγχου Τηλεπικοινωνιακού Παρόχου Κινητών Υπηρεσιών

Η διαδικασία ελέγχου παρόχου διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με Απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένου παρόχου. Η ελαχίστη στελέχωση της ομάδας ελέγχου περιλαμβάνει τον υπεύθυνο της ομάδας, έναν νομικό σύμβουλο και έναν τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η ομάδα ελέγχου, επικοινωνεί με τον πάροχο και ζητεί να έρθει σε άμεση επικοινωνία με τον υπεύθυνο ασφάλειας όπως αυτός ορίζεται στο κεφάλαιο IV του παρόντος. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με τον υπεύθυνο ασφάλειας καταγράφεται και φέρει τις ανάλογες κυρώσεις.

(γ) Ο υπεύθυνος ασφάλειας παραδίδει στην ομάδα ελέγχου πλήρες αντίγραφο της ΠΔΑΚΤΥ και των τυχών συνοδευτικών εγγράφων. Από τα παραδιδόμενα έγγραφα θα πρέπει να προκύπτουν οι ημερομηνίες έκδοσης και έγκρισης των συγκεκριμένων πολιτικών. Τυχόν καθυστέρηση επίδοσης σημειώνεται και φέρει τις ανάλογες κυρώσεις.

(δ) Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων ώστε να καταγραφούν οι τυχόν ελλείψεις που παρουσιάζονται στην πολιτική του παρόχου. Κατά την διαδικασία αυτή δύναται να ζητηθεί η συνδρομή του παρόχου έτσι ώστε να διασαφηνιστούν τυχόν ασάφειες και προβλήματα που παρουσιάζονται στην πολιτική προστασίας του απορρήτου.

(ε) Κατά την διάρκεια του ελέγχου ο πάροχος δεν έχει την δυνατότητα να αντικαταστήσει την πολιτική προστασίας του απορρήτου με νέα ούτε να προβεί σε τυχόν διορθώσεις αυτής.

(στ) Σε περίπτωση ασαφειών ως προς την πολιτική προστασίας του απορρήτου οι πάροχοι, μετά από σχετική σύσταση της ΑΔΑΕ θα προβαίνουν στις απαραίτητες διορθώσεις στην πολιτική τους

(ζ) Η ομάδα ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων του παρόχου για να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται από τα προσκομισθέντα έγγραφα. Η αυτοψία δύναται να περιλαμβάνει και επαφή με το προσωπικό του παρόχου. Η ομάδα ελέγχου καταγράφει αναλυτικά τις ελλείψεις και τα σφάλματα που τυχόν διαπιστώνονται.

(η) Ο πάροχος οφείλει να υποβάλλει στην ομάδα ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο από την ομάδα για την επιτυχή ολοκλήρωση του ελέγχου.

(θ) Τυχόν διαπίστωση έλλειψης συνεργασίας από τον πάροχο ή/και προσπάθειας παραπλάνησης της ομάδας ελέγχου καταγράφεται και φέρει τις ανάλογες κυρώσεις.

ΠΑΡΑΡΤΗΜΑ Β

Ελάχιστο περιεχόμενο του εντύπου με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Τηλεπικοινωνιακό Πάροχο αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Κινητών Τηλεπικοινωνιακών Υπηρεσιών»

Το ως άνω έντυπο θα περιέχει απαραιτήτως τουλάχιστον τα ακόλουθα στοιχεία:

(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.

(β) Τα ονοματεπώνυμα και της ιδιότητες των στελεχών της ΑΔΑΕ που απαρτίζουν την ομάδα ελέγχου καθώς και την ημερομηνία σύστασής της.

(γ) Το όνομα του υπό έλεγχο παρόχου καθώς και το όνομα του υπευθύνου ασφάλειας του.

(δ) Το χρόνο που απαιτήθηκε έως ότου να παραδοθεί στην ομάδα ελέγχου η πλήρης πολιτική διασφάλισης απορρήτου του παρόχου.

(ε) Ημερολόγιο ενεργειών και ερωτήσεων της ομάδας ελέγχου και καταγραφή της ανταπόκρισης του ελεγχόμενου παρόχου.

(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής της Πολιτικής Διασφάλισης της Προστασίας του Απορρήτου με καταγραφή τυχόν ελλείψεων και ασαφειών.

(ζ) Τις ημερομηνίες έναρξης και περάτωσης του ελέγχου.

(η) Τελικό πόρισμα του ελέγχου και εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 12 Νοεμβρίου 2004

Ο Πρόεδρος
ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ

Αριθ. 630 α (2)

Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)

Έχοντας υπόψη:

α. Το Ν. 3115/27.2.2003 άρθρο 1 παραγρ. 1.

β. Το Ν. 3115/27.2.2003, άρθρο 6 παραγρ. 1.

γ. Ότι εκ της παρούσης Απόφασης δεν προκύπτει δαπάνη για το Δημόσιο.

γ. Τη σχετική εισήγηση της Υπηρεσίας, αποφάσισε:

Κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση Απορρήτου κατά την παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

Σκοπός του παρόντος Κανονισμού είναι:

1. Η θέσπιση των υποχρεώσεων των παρόχων σταθερών τηλεπικοινωνιακών υπηρεσιών για τη διασφάλιση του απορρήτου των σταθερών τηλεπικοινωνιακών υπηρεσιών στα πλαίσια της σχετικής Νομοθεσίας (Ν. 2225/1994 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/2003 «Περί Διασφάλισης του Απορρήτου των Επικοινωνιών») και

2. Ο καθορισμός της διαδικασίας ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του παρόντος Κανονισμού υπάγονται όλοι οι τηλεπικοινωνιακοί πάροχοι, οι οποίοι παρέχουν ή συμμετέχουν στην παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών.

Άρθρο 2
Ορισμοί

Για τις ανάγκες του παρόντος Κανονισμού χρησιμοποιούνται οι παρακάτω ορισμοί.

Ακεραιότητα: Η επιβεβαίωση ότι τα δεδομένα τα οποία έχουν σταλεί, έχουν παραληφθεί ή αποθηκευτεί είναι πλήρη και αμετάβλητα.

Αντίγραφα ασφάλειας: Τα αντίγραφα των ηλεκτρονικών αρχείων πληροφοριών που αφορούν σε δεδομένα Επικοινωνίας και χρησιμοποιούνται σε περιπτώσεις καταστροφής των πρωτευόντων αρχείων για την ανάκτησή τους.

Απειλή: Η εν δυνάμει παραβίαση της ασφάλειας ενός συστήματος.

Αυθεντικότητα: Η επιβεβαίωση της εγκυρότητας της ταυτότητας.

Δεδομένα θέσης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία στο τηλεπικοινωνιακό δίκτυο και υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας.

Δεδομένα κίνησης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία για να επιτευχθεί η επικοινωνία μέσω του τηλεπικοινωνιακού δικτύου ή για την τιμολόγησή της.

Δημόσιες τηλεπικοινωνιακές υπηρεσίες: Οι τηλεπικοινωνιακές υπηρεσίες που διατίθενται στο κοινό.

Σταθερό τηλεπικοινωνιακό δίκτυο: Τηλεπικοινωνιακό δίκτυο, στο οποίο οι συνδρομητικές γραμμές είναι, στο ακραίο τμήμα τους, γραμμές σταθερών χάλκινων καλωδιακών δικτύων.

Δημόσιο τηλεπικοινωνιακό δίκτυο: Το τηλεπικοινωνιακό δίκτυο, που χρησιμοποιείται εν μέρει ή εν όλω, για την παροχή διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών. Όπου στο κείμενο αναφέρεται ο όρος «τηλεπικοινωνιακό δίκτυο» θα εννοείται το δημόσιο σταθερό τηλεπικοινωνιακό δίκτυο.

Έλεγχος πρόσβασης: Η πρόληψη μη εξουσιοδοτημένης χρήσης ενός πόρου, συμπεριλαμβανομένης της πρόληψης της χρήσης του πόρου με μη εξουσιοδοτημένο τρόπο.

Εμπιστευτικότητα: Η προστασία των επικοινωνιών ή των αποθηκευμένων δεδομένων από την υποκλοπή και την ανάγνωση από μη εξουσιοδοτημένα άτομα.

Εξουσιοδότηση: Η διαδικασία χορήγησης δικαιώματος

πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητείται η πρόσβαση.

Επίθεση: Οι δραστηριότητες που αποσκοπούν την παράκαμψη ή την εκμετάλλευση των ατελειών των μηχανισμών ασφάλειας ενός συστήματος. Διακρίνονται σε άμεσες (εκμετάλλευση ατελειών αλγορίθμων, αρχών και ιδιοτήτων του μηχανισμού ασφάλειας) και έμμεσες επιθέσεις (εξαναγκασμός του συστήματος να χρησιμοποιήσει το μηχανισμό ασφάλειας με λανθασμένο τρόπο ή παράκαμψη μηχανισμών).

Επικοινωνία: Κάθε είδους επικοινωνία μεταξύ ανθρώπων, αντικειμένων, ανθρώπων και αντικειμένων η οποία γίνεται είτε με τη μορφή του προφορικού ή γραπτού λόγου, είτε με τη μορφή μουσικής, ήχων και εικόνων, είτε με τη μορφή σημάτων είτε και με οποιοδήποτε συνδυασμό όλων αυτών των μορφών.

Προστασία του απορρήτου: Η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων Επικοινωνίας από άλλα πρόσωπα, χωρίς την συγκατάθεσή τους, εξαιρουμένων των νόμιμα εξουσιοδοτημένων.

Σταθερές τηλεπικοινωνιακές υπηρεσίες: Οι υπηρεσίες των οποίων η παροχή συνίσταται συνολικά ή εν μέρει στη μετάδοση και δρομολόγηση σημάτων μέσω σταθερών τηλεπικοινωνιακών δικτύων, εξαιρουμένων των ραδιοφωνικών και τηλεοπτικών εκπομπών.

Συνδρομητής: Κάθε φυσικό η νομικό πρόσωπο που έχει συνάψει σύμβαση με πάροχο διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών για την παροχή των υπηρεσιών αυτών.

Ταυτότητα: Οι πληροφορίες που προσδιορίζουν τον χρήστη των υπηρεσιών τηλεπικοινωνιακού δικτύου με μοναδικό τρόπο.

Τηλεπικοινωνία: Η μεταφορά ήχων, σημάτων, εικόνων, δεδομένων, και εν γένει κάθε φύσης πληροφοριών μεταδιδόμενων εν όλω ή εν μέρει μέσω ενσύρματων, ασύρματων, ηλεκτρομαγνητικών, φωτοηλεκτρονικών ή φωτοοπτικών συστημάτων.

Τηλεπικοινωνιακός πάροχος: Φυσικό ή νομικό πρόσωπο που παρέχει τηλεπικοινωνιακές υπηρεσίες στο κοινό. Οπου στο κείμενο αναφέρεται ο όρος πάροχος χωρίς επεξήγηση θα εννοείται «τηλεπικοινωνιακός πάροχος».

Υπηρεσία κλήσης έκτακτης ανάγκης: Η υπηρεσία λήψης και διαχείρισης κλήσεων έκτακτης ανάγκης που γίνονται προς ένα καθορισμένο αριθμό κλήσης και δρομολογούνται προς ειδικές, κρατικές και μη, Υπηρεσίες όπως είναι η Αστυνομία, η Πυροσβεστική Υπηρεσία, τα Νοσοκομεία κ.λπ.

Χρήστης: Κάθε φυσικό πρόσωπο ή νομική οντότητα που χρησιμοποιεί ή ζητά να χρησιμοποιήσει διαθέσιμη στο κοινό τηλεπικοινωνιακή υπηρεσία.

Χρήστης Παρόχου: Κάθε φυσικό πρόσωπο που ανήκει στο προσωπικό ή τους συνεργάτες του Παρόχου και χρησιμοποιεί τα συστήματα και τις υποδομές του Παρόχου.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΣΤΑΘΕΡΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 3
Ορισμός - Γενικές Απαιτήσεις και Συστάσεις

1. Πολιτική Διασφάλισης του Απορρήτου των Σταθερών Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΣΤΥ) είναι το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου της τηλεπικοινωνίας μέσω σταθερών δικτύων.

2. Η ΠΔΑΣΤΥ θα εκπονείται από τους τηλεπικοινωνιακούς παρόχους διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών με βάση τις απαιτήσεις και τις υποδείξεις του παρόντος Κανονισμού και θα εφαρμόζεται από αυτούς μετά την έγκρισή της από την ΑΔΑΕ.

3. Η ΠΔΑΣΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική προστασίας τηλεπικοινωνιακών δικτύων, η Πολιτική επεξεργασίας δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το προσωπικό και τους συνεργάτες των τηλεπικοινωνιακών παρόχων, η Πολιτική πρόσβασης, η Πολιτική αποδεκτής χρήσης και η Πολιτική άρσης του απορρήτου, από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λειτουργία, τη διαχείριση και τη χρήση των τηλεπικοινωνιακών υπηρεσιών.

4. Η ΠΔΑΣΤΥ για να θεωρείται επαρκής θα πρέπει να διαθέτει τουλάχιστον τα ακόλουθα χαρακτηριστικά:

α) Να υλοποιείται μέσω διαδικασιών διαχείρισης συστημάτων, δημοσιοποίησης οδηγιών αποδεκτής χρήσης ή άλλων αντίστοιχων κατάλληλων μεθόδων.

β) Οι διαδικασίες, οι οποίες σχετίζονται με την υλοποίηση της πολιτικής, πρέπει να περιλαμβάνουν τουλάχιστον τον προσδιορισμό ταυτότητας, την αυθεντικότητα, την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εμπιστευτικότητα, την ακεραιότητα, την προστασία του απορρήτου και τον έλεγχο παραβίασης του απορρήτου.

γ) Να εφαρμόζεται μέσω εργαλείων ασφάλειας ή/και μέσω διαδικασιών ασφαλείας.

δ) Να καθορίζει τις περιοχές ευθύνης των χρηστών και των χρηστών παρόχου. Επιπλέον οι μηχανισμοί μεταβολής της πολιτικής διασφάλισης του απορρήτου πρέπει να είναι προσδιορισμένοι με σαφήνεια, περιλαμβάνοντας τη διαδικασία, τους εμπλεκόμενους, καθώς και τους υπεύθυνους προς έγκριση.

5. Επίσης, συνιστάται η ΠΔΑΣΤΥ:

α) Να είναι ανεξάρτητη, στο μέτρο που είναι δυνατόν από τεχνικής απόψεως, από συγκεκριμένο εξοπλισμό (υλικό, λογισμικό) και

β) Να βασίζεται σε μια ανοικτή αρχιτεκτονική ώστε να καθίσταται βιώσιμη μακροπρόθεσμα.

6. Η ΠΔΑΣΤΥ υπόκειται σε έλεγχο από την ΑΔΑΕ, τόσο όσο ως προς την πληρότητα και αποτελεσματικότητα της, όσο και ως προς το βαθμό εφαρμογής της.

Άρθρο 4
Χάραξη και στοιχεία Πολιτικής Διασφάλισης Απορρήτου Σταθερών Τηλεπικοινωνιακών Υπηρεσιών

1. Ένας τηλεπικοινωνιακός πάροχος, προκειμένου να χαράξει την πολιτική του, μπορεί, χωρίς να υποχρεώνεται ή να περιορίζεται, να ακολουθήσει τα παρακάτω βήματα:

α) Να προσδιορίσει τις πληροφορίες που πρέπει να προστατευτούν.

β) Να προσδιορίσει τα ευάλωτα σημεία του τηλεπικοινωνιακού δικτύου.

γ) Να προσδιορίσει τους κινδύνους και τις απειλές για τα α), β).

δ) Να προσδιορίσει τα μέτρα διασφάλισης της προστασίας του απορρήτου στις σταθερές τηλεπικοινωνιακές υπηρεσίες.

ε) Να καθορίσει τις υποχρεώσεις των υπαλλήλων και συνεργατών του.

στ) Να καθορίσει τις δεσμεύσεις και υποχρεώσεις του έναντι των πελατών του και

ζ) να καταρτίσει σχέδιο αναθεώρησης και βελτίωσης της ΠΔΑΣΤΥ κάθε φορά που θα εντοπίζεται νέος κίνδυνος ή αδυναμία ή που θα προκύπτουν νέες τεχνολογικές διευκολύνσεις διαχείρισης ασφάλειας.

2. Κάθε τηλεπικοινωνιακός πάροχος πρέπει, εν ανάγκη σε συνεργασία με τους παρόχους τηλεπικοινωνιακού δικτύου, να τεκμηριώνει με σχέδια την προστασία του απορρήτου για να αντιμετωπίσει προβλήματα που πιθανόν να εμφανισθούν σε έκτακτες περιστάσεις, όπως είναι η άρση του απορρήτου μετά από εντολή δικαστικών ή εισαγγελικών αρχών (Νόμος 2225) και η προβληματική λειτουργία των τηλεπικοινωνιακών ή/και των μηχανογραφικών συστημάτων του ή των συστημάτων των συνεργατών του.

Άρθρο 5
Πληροφορίες που πρέπει να προστατεύονται

1.Κάθε τηλεπικοινωνιακός πάροχος οφείλει να διασφαλίζει και να προστατεύει το απόρρητο των δεδομένων της επικοινωνίας, που χρησιμοποιείται για την παροχή της τηλεπικοινωνιακής υπηρεσίας, τη διεκπεραίωση της επικοινωνίας, κτλ. Ενδεικτικά αναφέρονται οι παρακάτω πληροφορίες που πρέπει να προστατεύονται, όσο ευρίσκονται στη δικαιοδοσία του παρόχου:

α) Ο αριθμός του καλούντος και του καλούμενου συνδρομητή.

β) Η ταυτότητα της τερματικής συσκευής.

γ) Τα στοιχεία του δικτύου.

δ) Ο αριθμός δρομολόγησης.

ε) Ο χρόνος διενέργειας και η διάρκεια της επικοινωνίας.

στ) Οι πληροφορίες καταλόγου (ονοματεπώνυμο συνδρομητή, διεύθυνση, αριθμός κτλ).

ζ) Η θέση του καλούντος ή/και του καλούμενου χρήστη γενικά και ειδικότερα στις περιπτώσεις καρτών χρονοχρέωσης, καρτοτηλεφώνων κτλ.

η) Τα στοιχεία χρέωσης της επικοινωνίας.

θ) Το περιεχόμενο της επικοινωνίας.

2. Οι πάροχοι σταθερών τηλεπικοινωνιακών υπηρεσιών θα πρέπει να προσδιορίζουν τους κινδύνους και τις ενδεχόμενες απειλές για τα παραπάνω στοιχεία. Ο πάροχος οφείλει να διασφαλίζει το απόρρητο της μετάδοσης και αποθήκευσης των δεδομένων Επικοινωνίας που χρησιμοποιούνται σε ένα δίκτυο σταθερών επικοινωνιών. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να ενημερώνει τους χρήστες του με συγκεκριμένους τρόπους και μέσα της επιλογής του για οποιουσδήποτε ειδικούς κινδύνους σχετικά με την ασφάλεια των υπηρεσιών που παρέχει καθώς επίσης και οποιωνδήποτε δυνατοτήτων για την απομάκρυνση των κινδύνων και του κόστους των μέτρων που περιλαμβάνονται.

Άρθρο 6
Ευάλωτα Σημεία Σταθερού Τηλεπικοινωνιακού Δικτύου

Ενδεικτικά αναφέρονται τα ευάλωτα σε επιθέσεις σημεία του δικτύου:

1. Στοιχεία τερματικών συσκευών χρηστών:

α) Η τηλεφωνική συσκευή.

β) Το σημείο σύνδεσης του τηλεφώνου (ροζέτα ή πρίζα).

γ) Τυχόν ενσωματωμένος αυτόματος τηλεφωνητής.

δ) Η διάταξη τερματισμού (NT) σύνδεσης ISDN.

ε) Ο σταθμός βάσης των κοινών ασύρματων τηλεφώνων.

στ) Οι διατάξεις modem στην IP επικοινωνία και τη σύνδεση με δίκτυα δεδομένων.

ζ) Οι συσκευές τηλεειδοποίησης.

2. Στοιχεία δικτύου και υπηρεσιών:

α) Ο κύριος και δευτερεύων κατανεμητής εσωτερικού δικτύου (Εσκαλίτ).

β) Το κυτίο διανομής (Box).

γ) Οι υπαίθριοι κατανεμητές καλωδίων (KV).

δ) Τα συνδρομητικά κέντρα και τα ιδιωτικά δίκτυα.

ε) Οι εσωτερικές καλωδιώσεις τοπικών δικτύων.

στ) Οι διακομιστές (servers).

ζ) Το φωνητικό ταχυδρομείο (Voice mail).

η) Τα κέντρα μεταγωγής.

θ) Οι κεντρικοί κατανεμητές.

Ο Τηλεπικοινωνιακός Πάροχος θα πρέπει να ενημερώνει τους χρήστες για τα ευάλωτα σημεία που ανήκουν στη περιοχή ευθύνης τους και να λαμβάνει όλα τα προσήκοντα μέτρα για την προστασία των ευάλωτων σημείων που ανήκουν στην δικαιοδοσία του.

ΚΕΦΑΛΑΙΟ III
ΕΠΙ ΜΕΡΟΥΣ ΠΟΛΙΤΙΚΕΣ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΣΤΑΘΕΡΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 7
Προστασία Τηλεπικοινωνιακών Δικτύων

1. Η ασφάλεια ενός τηλεπικοινωνιακού δικτύου περιλαμβάνει: α) την προστασία από απειλές που οφείλονται σε ενδογενείς αδυναμίες αξιοπιστίας του δικτύου, και β) την ευαισθησία του σε απειλές οφειλόμενες σε αδυναμίες διασυνδεομένων δικτύων ή τερματικών και γ) την δυνατότητα αντιμετώπισης εξωτερικών επιθέσεων.

2. Η ασφάλεια αυτή επιτυγχάνεται με κατάλληλο συνδυασμό ανθεκτικότητας, εφεδρικότητας, αποκατάστασης και επισκευής. Τούτο μπορεί να πραγματοποιηθεί με τη χρησιμοποίηση αξιόπιστου εξοπλισμού και δικτυακής αρχιτεκτονικής που θα διασφαλίζουν το δίκτυο από εσωτερικές και εξωτερικές απειλές και θα το καθιστούν ικανό να ανταποκριθεί με ταχύτητα και αποτελεσματικότητα στην αντιμετώπιση πιθανών βλαβών που μπορεί να υποστεί το σύστημα ασφάλειας των υπηρεσιών του.

3. Κάθε τηλεπικοινωνιακός πάροχος, προκειμένου να χαράξει και να εφαρμόσει την πολιτική προστασίας του τηλεπικοινωνιακού δικτύου που χρησιμοποιεί, οφείλει, εν ανάγκη και με τη συνεργασία των συνεργαζομένων με αυτόν παρόχων τηλεπικοινωνιακού δικτύου, να εντοπίζει με σχολαστικότητα όλα τα σημεία του δικτύου που απειλούνται και να εξαντλεί κάθε δυνατότητα πλήρους διασφάλισής τους. Ορισμένα από τα σημεία αυτά αναφέρονται στην παραπάνω παράγραφο 6.

4. Για την εκπόνηση μιας επαρκούς πολιτικής ασφάλειας του δικτύου έναντι επιθέσεων και άλλων μορφών φυσικών παρεμβάσεων συνιστάται:

α) Να λαμβάνονται τα απαραίτητα μέτρα για τη σωστή χωροθέτηση του τηλεπικοινωνιακού εξοπλισμού των τηλεφωνικών κέντρων, την προστασία των δικτυακών εγκαταστάσεων (συνδρομητικών και ζευκτικών γραμμών, τερματικών σταθμών, σταθμών βάσης, κεραιών, συστημάτων μετάδοσης, κατανεμητών κτλ).

β) Να αξιοποιούνται οι δυνατότητες της σηματοδοσίας για έλεγχο και διασφάλιση των μεταδιδομένων πληροφοριών και των δεδομένων κίνησης.

γ) Ο αριθμός των σημείων διασύνδεσης με άλλα δίκτυα

να είναι ο ενδεικνυόμενος ώστε ο έλεγχός τους να είναι ευχερέστερος, ευρύτερος και οικονομικότερος.

δ) Η τοποθέτηση των κοινόχρηστων τηλεφώνων καθώς και των τηλεφωνικών θαλάμων να γίνεται σε περιοχές κατά το δυνατόν ασφαλέστερες έτσι ώστε να ελαχιστοποιείται ο κίνδυνος παραβίασής τους.

Άρθρο 8
Προστασία Επεξεργασίας των Δεδομένων Επικοινωνίας

Οι τηλεπικοινωνιακοί πάροχοι οφείλουν να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της κείμενης νομοθεσίας για την προστασία της επεξεργασίας των δεδομένων Επικοινωνίας.

Άρθρο 9
Ασφάλεια σε σχέση με τους Χρήστες Παρόχου

1. Οι χρήστες παρόχου οφείλουν να συμμορφώνονται με τις διατάξεις της νομοθεσίας περί προστασίας του απορρήτου.

Ειδικότερα τα εν λόγω πρόσωπα απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που αφορούν: i) τα περιεχόμενα ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω παρόχου υπηρεσιών επικοινωνιών ή ii) τις υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα άλλο πρόσωπο μέσω ενός παρόχου υπηρεσιών σταθερών επικοινωνιών ή iii) τα δεδομένα Επικοινωνίας ενός άλλου χρήστη (όπως μη ανακοινώσιμα τηλέφωνα και διευθύνσεις) και υποπίπτουν στην αντίληψη ή στην κατοχή του, ως αποτέλεσμα της φύσης της εργασίας του.

2. Οι χρήστες παρόχου που διαχειρίζονται κλήσεις έκτακτης ανάγκης απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που αφορούν: i) τα περιεχόμενα ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω του τηλεπικοινωνιακού παρόχου ή ii) τα δεδομένα Επικοινωνίας ενός άλλου χρήστη (όπως μη ανακοινώσιμες συνδέσεις και διευθύνσεις) που υποπίπτουν στην αντίληψη ή στην κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

3. Οι τυχόν αναγκαίες εξαιρέσεις των προηγούμενων γενικών κανόνων θα περιγράφονται με σαφήνεια στην πολιτική ασφάλειας του τηλεπικοινωνιακού παρόχου.

Άρθρο 10
Πολιτική Πρόσβασης

1. Η Πολιτική Πρόσβασης καθορίζει το επίπεδο πρόσβασης χρηστών παρόχου και διεργασιών λογισμικού σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου.

2. Η Πολιτική Πρόσβασης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΣΤΥ.

3. Ο πάροχος οφείλει να διαθέτει και να εφαρμόζει Πολιτική Πρόσβασης για όλα τα συστήματα που αποτελούν τον εξοπλισμό του, όπως π.χ. εξωτερικές διατάξεις σύνδεσης, συστήματα μεταγωγής και μετάδοσης τηλεπικοινωνιακών πληροφοριών, τερματικές διατάξεις, μηχανογραφικούς εξοπλισμούς (υλικού και λογισμικού) κτλ.

4. Για κάθε σύστημα θα περιγράφονται, με τρόπο λεπτομερή και σαφή, τουλάχιστον οι ακόλουθες διαδικασίες:

α) Διαδικασίες προσθήκης νέων συνδρομητών και χρηστών στο σύστημα.

β) Διαδικασίες εξουσιοδότησης σχετικά με την προσθήκη, διαγραφή και αλλαγή των επιπέδων πρόσβασης των χρηστών παρόχου σε τηλεπικοινωνιακές υπηρεσίες του συστήματος.

γ) Διαδικασίες ταυτοποίησης χρηστών.

δ) Διαδικασίες ελέγχου των παραπάνω διαδικασιών και διαχείρισης του επιπέδου πρόσβασης που παραχωρείται στους χρήστες παρόχου.

ε) Διαδικασίες πρόσβασης χρηστών παρόχου σε συστήματα που διατηρούν δεδομένα κίνησης και θέσης χρηστών.

στ) Σε περίπτωση που χρησιμοποιείται κρυπτογράφηση, η Πολιτική Πρόσβασης θα πρέπει να περιέχει τις διαδικασίες πρόσβασης χρηστών παρόχου σε συστήματα κρυπτογράφησης / αποκρυπτογράφησης καθώς και σε διαδικασίες σχετικά με την διαχείριση, διανομή, εισαγωγή και αρχειοθέτηση των κλειδιών κρυπτογράφησης. Οι πληροφορίες αυτές θα αναφέρονται σε καταλλήλως διαβαθμισμένο παράρτημα των εγγράφων που καθορίζουν την Πολιτική Πρόσβασης.

Άρθρο 11
Πολιτική Αποδεκτής Χρήσης

1. Η Πολιτική Αποδεκτής Χρήσης περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών και χρηστών παρόχου των τηλεπικοινωνιακών συστημάτων ενός παρόχου.

2. Η Πολιτική Αποδεκτής Χρήσης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΣΤΥ.

3. Σκοπός της είναι να διασφαλίσει ότι οι χρήστες και οι χρήστες παρόχου δεν θα εκμεταλλευτούν την πρόσβαση που τους παρέχεται σύμφωνα με την Πολιτική Πρόσβασης σε παντός είδους τηλεπικοινωνιακά δίκτυα προκειμένου να προβούν σε ενέργειες μη επιτρεπόμενες σύμφωνα με τη νομοθεσία και τον παρόντα Κανονισμό.

4. Η Πολιτική Αποδεκτής Χρήσης πρέπει να είναι προσαρμοσμένη στην κατηγορία χρηστών στην οποία απευθύνεται (χρηστών και χρηστών παρόχου) και να είναι σύμφωνη με την Πολιτική Πρόσβασης για κάθε κατηγορία χρηστών.

5. Στην Πολιτική Αποδεκτής Χρήσης θα πρέπει, με όσο το δυνατόν πιο λεπτομερή και κατανοητό τρόπο ώστε να αποφεύγονται οι παρερμηνείες, να περιλαμβάνονται κατ' ελάχιστον τα ακόλουθα:

α) Τα δικαιώματα του χρήστη και του χρήστη παρόχου. Σε αυτή την ενότητα θα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης.

β) Οι υποχρεώσεις του χρήστη και του χρήστη παρόχου. Σε αυτή την ενότητα θα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα μη αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης, καθώς και οι συνέπειες της μη συμμόρφωσης με αυτές τις υποχρεώσεις.

γ) Τα δικαιώματα του τηλεπικοινωνιακού παρόχου.

δ) Οι υποχρεώσεις του τηλεπικοινωνιακού παρόχου.

6. Επιπλέον στην ενότητα που αναφέρεται στις υποχρεώσεις των χρηστών, η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει τις παρακάτω διατάξεις οι οποίες σχετίζονται με την ασφάλεια του συστήματος:

α) Οι χρήστες οφείλουν να λαμβάνουν όλα τα ενδεικνυόμενα μέτρα για την διασφάλιση του απορρήτου επικοινωνιών τους.

β) Οι χρήστες οφείλουν να ενημερώνουν αμέσως τους υπευθύνους του παρόχου αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέ-

τει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών.

γ) Οι χρήστες οφείλουν να αποκτούν πρόσβαση αποκλειστικά και μόνο σε δεδομένα κίνησης ή θέσης τα οποία αναφέρονται στους ίδιους ή είναι δημοσίως ανακοινώσιμα ή για τα οποία τους έχει δοθεί δυνατότητα πρόσβασης σύμφωνα με την Πολιτική Πρόσβασης.

δ) Οι χρήστες απαγορεύεται να επιχειρούν να εκμεταλλευτούν πιθανά κενά ασφάλειας των συστημάτων του παρόχου προκειμένου να αποκτήσουν πρόσβαση σε πληροφορίες άλλων χρηστών, να διαταράξουν την ομαλή λειτουργία των δικτύων, να εκτελέσουν κακόβουλο λογισμικό και γενικά να υποβαθμίσουν το επίπεδο ασφάλειας του συστήματος με σκοπό να παραβιάσουν την προστασία του απορρήτου.

7. Ο πάροχος οφείλει να δίνει στον χρήστη πρόσβαση στα συστήματά του μόνο εφόσον ο χρήστης έχει λάβει γνώση και έχει αποδεχθεί την Πολιτική Αποδεκτής Χρήσης. Το γεγονός αυτό αποδεικνύεται είτε με έγγραφη δήλωση του χρήστη η οποία φέρει την πρωτότυπη υπογραφή του ή εφόσον ο χρήστης έχει συμπληρώσει το αντίστοιχο πεδίο σε σχετική φόρμα αποδοχής στην περίπτωση που η Πολιτική Αποδεκτής Χρήσης παρουσιάζεται ηλεκτρονικά.

ΚΕΦΑΛΑΙΟ IV
ΥΠΟΧΡΕΩΣΕΙΣ ΠΑΡΟΧΩΝ - ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 12
Υποχρεώσεις Παρόχων Σταθερών Τηλεπικοινωνιακών Υπηρεσιών

1. Όλοι οι τηλεπικοινωνιακοί πάροχοι υποχρεούνται:

α) Να διαθέτουν ανά πάσα στιγμή καθορισμένη πολιτική για τη διασφάλιση του απορρήτου τηλεπικοινωνιακών υπηρεσιών παρεχομένων από δημόσια σταθερά τηλεπικοινωνιακά δίκτυα.

β) Να εφαρμόζουν την εν λόγω πολιτική.

γ) Να ενημερώσουν σχετικά ως προς την εφαρμοζόμενη πολιτική την ΑΔΑΕ εντός έξι μηνών από την δημοσίευση του παρόντος.

δ) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική εντός ενός έτους από την έγκρισή της.

2. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβλέπει στο οργανόγραμμά του ξεχωριστή διοικητική οντότητα, η οποία θα είναι επιφορτισμένη με την κατάρτιση και την εφαρμογή της ΠΔΑΣΤΥ με επικεφαλής κατάλληλα καταρτισμένο στέλεχός του που θα φέρει τον τίτλο του Υπευθύνου Ασφαλείας.

3. Για την αποτελεσματική εφαρμογή της Πολιτικής Πρόσβασης ο κάθε τηλεπικοινωνιακός πάροχος οφείλει να ορίζει τουλάχιστον:

α) Έναν Υπεύθυνο Πρόσβασης, ο οποίος θα καθορίζει το είδος της πρόσβασης των χρηστών στα συστήματα.

β) Έναν Υπεύθυνο Συστήματος, ο οποίος θα υλοποιεί τις αποφάσεις του Υπευθύνου Πρόσβασης.

γ) Έναν Υπεύθυνο Αντιγράφων Ασφαλείας, ο οποίος πάντα σε συνεννόηση με τον Υπεύθυνο Πρόσβασης θα καθορίζει ποιος έχει πρόσβαση στα αντίγραφα ασφάλειας καθώς και κάθε πότε θα λαμβάνονται αντίγραφα ασφάλειας και για ποια δεδομένα.

4. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβαίνει σε τακτικές επισκοπήσεις και αναθεωρήσεις της πολιτικής διασφάλισης του απορρήτου, είτε αυτόβουλα (μετά από έγκριση της ΑΔΑΕ σε περίπτωση αναθεώρησης) είτε ύστερα από σχετική εντολή της ΑΔΑΕ όπως μπορεί να προκύψει από πιθανή διαδικασία ελέγχου ή έκδοση σχετικής οδηγίας.

5. Σε περίπτωση πιθανής παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου, ο πάροχος οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους) και να παρέχει στοιχεία για την αποτροπή ή αντιμετώπισή τους.

6. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου που δεν είναι δυνατό να αντιμετωπιστεί με τα τρέχοντα μέσα που διαθέτει ο τηλεπικοινωνιακός πάροχος, οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους).

7. Ο πάροχος οφείλει να ενημερώνει τους χρήστες για την ύπαρξη και τον τρόπο χρήσης τεχνολογιών - πόρων σχετικών με ασφάλεια των μεταδιδόμενων πληροφοριών (π.χ. Secure Shell Server, SSH)

8. Ο πάροχος οφείλει να ορίζει και να γνωστοποιεί στους συνδρομητές του τις συνέπειες για τη μη συμμόρφωση των χρηστών παρόχου με τα προβλεπόμενα από την Πολιτική Διασφάλισης του Απορρήτου (συμπεριλαμβανομένων των Πολιτικών Πρόσβασης και Αποδεκτής Χρήσης).

Άρθρο 13
Διαδικασία Ελέγχου από την ΑΔΑΕ-Κυρώσεις

1. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του παρόντος. Η συχνότητα των ελέγχων θα καθοριστεί από την ΑΔΑΕ με μεταγενέστερη Απόφασή της.

2. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες υπηρεσίες της ΑΔΑΕ ή από ειδικούς που τελούν υπό την άμεση επίβλεψη της ΑΔΑΕ, με την παρουσία εξουσιοδοτημένου προσώπου του παρόχου, σύμφωνα με τη διαδικασία που περιγράφεται στο Παράρτημα Α του παρόντος Κανονισμού.

3. Κατά την διάρκεια του ελέγχου η ΑΔΑΕ καταγράφει αναλυτικά τις ενέργειες σε ειδικό έντυπο με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Πάροχο Σταθερών Τηλεπικοινωνιακών Υπηρεσιών αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Σταθερών Τηλεπικοινωνιακών Υπηρεσιών». Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β του παρόντος Κανονισμού.

4. Η ομάδα ελέγχου κοινοποιεί το πόρισμά της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου λαμβάνοντας υπόψη και τις πιθανές ενστάσεις του παρόχου και είτε εγκρίνει τις ενέργειες που προβλέπονται στην εκάστοτε πολιτική προστασίας του απορρήτου του παρόχου που έχει εγκριθεί από την ΑΔΑΕ είτε επιβάλλει κυρώσεις εφόσον κρίνει ότι δεν έχουν ληφθεί τα προσήκοντα μέτρα, με βάση τα αναφερόμενα στην εγκεκριμένη ΠΔΑΣΤΥ.

5. Η ΑΔΑΕ διενεργεί έκτακτους ελέγχους σε περίπτωση δημόσιων καταγγελιών ή έγγραφων καταγγελιών εκ μέρους των χρηστών. Εφόσον πρόκειται για δημόσιες καταγγελίες, ακολουθείται η διαδικασία που προβλέπεται για τους τακτικούς ελέγχους, ενώ στην περίπτωση εμπιστευτικών έγγραφων καταγγελιών εκ μέρους χρηστών, ο έλεγχος μπορεί κατά την κρίση της ΑΔΑΕ να γίνει αιφνιδιαστικά.

6. Ως προς τη διαδικασία και τις κυρώσεις της παρα-

γράφου 5, ισχύουν οι διατάξεις του Νόμου 3115, άρθρο 11 και άρθρο 6, παράγραφος 4, καθώς και τα προβλεπόμενα στον εσωτερικό κανονισμό της ΑΔΑΕ (ΦΕΚ 1642/Β/7.11.2003).

Άρθρο 14
Άσκηση Εποπτείας

1. Κάθε πάροχος στο τέλος του ημερολογιακού έτους υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν στην διασφάλιση του απορρήτου των σταθερών τηλεπικοινωνιακών υπηρεσιών.

2. Το ελάχιστο περιεχόμενο της ετήσιας έκθεσης ορίζεται ως εξής:

α) Περιστατικά που απείλησαν τη διασφάλιση του απορρήτου καθώς και τυχόν βλάβες που υπέστη ο πάροχος και οι χρήστες του εξαιτίας αυτών.

β) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της ετήσιας έκθεσης.

3. Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τους παρόχους οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στα πλαίσια των αρμοδιοτήτων της για τη διασφάλιση του απορρήτου.

Άρθρο 15
Προστασία Επεξεργασίας Αρχείων

Σε περιπτώσεις παραβίασης των διατάξεων προστασίας του απορρήτου των επικοινωνιών, οι οποίες περιλαμβάνουν και επεξεργασία αρχείων που αφορούν την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η ΑΔΑΕ θα την ενημερώνει σχετικά προκειμένου να επιλαμβάνεται στο πλαίσιο των δικών της αρμοδιοτήτων.

ΚΕΦΑΛΑΙΟ V
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 16
Έναρξη Ισχύος

Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α

Αναλυτική Περιγραφή Διαδικασίας Ελέγχου Παρόχου

Η διαδικασία ελέγχου παρόχου διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με Απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένου παρόχου. Η ελαχίστη στελέχωσης της ομάδας ελέγχου περιλαμβάνει έναν υπεύθυνο της ομάδας, έναν νομικό σύμβουλο και έναν τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η ομάδα ελέγχου, επικοινωνεί με τον πάροχο και ζητεί να έρθει σε άμεση επικοινωνία με τον υπεύθυνο ασφάλειας όπως αυτός ορίζεται στο κεφάλαιο IV του παρόντος. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με τον υπεύθυνο ασφάλειας καταγράφεται και φέρει τις ανάλογες κυρώσεις.

(γ) Ο υπεύθυνος ασφάλειας παραδίδει στην ομάδα ελέγχου πλήρες αντίγραφο της ΠΔΑΣΤΥ και των τυχόν συνοδευτικών εγγράφων. Από τα παραδιδόμενα έγγραφα θα πρέπει να προκύπτουν οι ημερομηνίες έκδοσης και έγκρισης των συγκεκριμένων πολιτικών. Τυχόν καθυστέρηση επίδοσης σημειώνεται και φέρει τις ανάλογες κυρώσεις.

(δ) Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων ώστε κα καταγραφούν οι τυχόν ελλείψεις που παρουσιάζονται στην πολιτική του παρόχου. Κατά την διαδικασία αυτή δύναται να ζητηθεί η συνδρομή του παρόχου έτσι ώστε να διασαφηνιστούν τυχόν ασάφειες και προβλήματα που παρουσιάζονται στην πολιτική προστασίας του απορρήτου.

(ε) Κατά την διάρκεια του ελέγχου ο πάροχος δεν έχει την δυνατότητα να αντικαταστήσει την πολιτική προστασίας του απορρήτου με νέα ούτε να προβεί σε τυχόν διορθώσεις αυτής.

(στ) Σε περίπτωση ασαφειών ως προς την πολιτική προστασίας του απορρήτου οι πάροχοι, μετά από σχετική σύσταση της ΑΔΑΕ θα προβαίνουν στις απαραίτητες διορθώσεις στην πολιτική τους.

(ζ) Η ομάδα ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων του παρόχου για να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται από τα προσκομιθέντα έγγραφα. Η αυτοψία δύναται να περιλαμβάνει και επαφή με το προσωπικό του παρόχου. Η ομάδα ελέγχου καταγράφει αναλυτικά τις ελλείψεις και τα σφάλματα που τυχόν διαπιστωθούν.

(η) Ο πάροχος οφείλει να υποβάλλει στην ομάδα ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο από την ομάδα για την επιτυχή ολοκλήρωση του ελέγχου.

(θ) Τυχόν διαπίστωση έλλειψης συνεργασίας από τον πάροχο ή/και προσπάθειας παραπλάνησης της ομάδας ελέγχου καταγράφεται και φέρει τις ανάλογες κυρώσεις.

ΠΑΡΑΡΤΗΜΑ Β

Ελάχιστο περιεχόμενο του εντύπου με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Τηλεπικοινωνιακό Πάροχο αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Σταθερών Τηλεπικοινωνιακών Υπηρεσιών»

Το ως άνω έντυπο θα περιέχει απαραιτήτως τουλάχιστον τα ακόλουθα στοιχεία:

(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.

(β) Τα ονοματεπώνυμα και της ιδιότητες των στελεχών της ΑΔΑΕ που απαρτίζουν την ομάδα ελέγχου καθώς και την ημερομηνία σύστασής της.

(γ) Το όνομα του υπό έλεγχο παρόχου καθώς και το όνομα του υπευθύνου ασφάλειας του.

(δ) Το χρόνο που απαιτήθηκε έως ότου να παραδοθεί στην ομάδα ελέγχου η πλήρης πολιτική διασφάλισης απορρήτου του παρόχου.

(ε) Ημερολόγιο ενεργειών και ερωτήσεων της ομάδας ελέγχου και καταγραφή της ανταπόκρισης του ελεγχόμενου παρόχου.

(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής της Πολιτικής Διασφάλισης της Προστασίας του Απορρήτου με καταγραφή τυχόν ελλείψεων και ασαφειών.

(ζ) Τις ημερομηνίες έναρξης και περάτωσης του ελέγχου.

(η) Τελικό πόρισμα του ελέγχου και εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 12 Νοεμβρίου 2004

Ο Πρόεδρος
ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ

Αριθ. 631 α

Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασυρμάτων Δικτύων.

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)

Έχοντας υπόψη:

α. Το Ν. 3115/27.2.2003 άρθρο 1 παραγρ. 1.

β. Το Ν. 3115/27.2.2003, άρθρο 6 παραγρ. 1.

γ. Ότι εκ της παρούσας Αποφάσεως δεν προκύπτει δαπάνη για το Δημόσιο.

γ. Τη σχετική εισήγηση της Υπηρεσίας, αποφάσισε:

Κατά τη συνεδρίασή της την 10η Νοεμβρίου 2004, την έγκριση του παρακάτω Κανονισμού για τη Διασφάλιση Απορρήτου κατά την παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασυρμάτων Δικτύων.

ΚΕΦΑΛΑΙΟ Ι
ΣΚΟΠΟΣ - ΟΡΙΣΜΟΙ

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

Σκοπός του παρόντος Κανονισμού είναι:

1. Η θέσπιση των υποχρεώσεων των φορέων παροχής τηλεπικοινωνιακών υπηρεσιών μέσω ασυρμάτων δικτύων για τη διασφάλιση του απορρήτου αυτών στα πλαίσια της σχετικής Νομοθεσίας (Ν. 2225/1994 «Περί προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Ν. 3115/2003 «Περί Διασφάλισης του Απορρήτου των Επικοινωνιών»).

2. Η παρουσίαση βασικών χαρακτηριστικών ασφαλείας των τεχνολογιών ασυρμάτων δικτύων.

3. Ο καθορισμός των διαδικασιών ελέγχου στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλοι οι πάροχοι τηλεπικοινωνιακών υπηρεσιών μέσω ασυρμάτων δικτύων.

Άρθρο 2
Ορισμοί

Για τις ανάγκες του παρόντος Κανονισμού χρησιμοποιούνται οι παρακάτω ορισμοί.

Ακεραιότητα: Η επιβεβαίωση ότι τα δεδομένα τα οποία έχουν σταλεί, έχουν παραληφθεί ή έχουν αποθηκευθεί είναι πλήρη και αμετάβλητα.

Αντίγραφα ασφάλειας:Τα αντίγραφα των ηλεκτρονικών αρχείων πληροφοριών που αφορούν σε δεδομένα Επικοινωνίας και χρησιμοποιούνται σε περιπτώσεις καταστροφής των πρωτευόντων αρχείων για την ανάκτησή τους.

Απειλή: Η εν δυνάμει παραβίαση της ασφάλειας ενός συστήματος.

Αυθεντικότητα: Η επιβεβαίωση της εγκυρότητας της ταυτότητας.

Δεδομένα θέσης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία στο τηλεπικοινωνιακό δίκτυο υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας.

Δεδομένα κίνησης: Όλες οι πληροφορίες που υποβάλλονται σε επεξεργασία για την αποκατάσταση επικοινωνίας μέσω του τηλεπικοινωνιακού δικτύου ή για την τιμολόγησή της.

Πιστοποιημένες συσκευές: Οι συσκευές που έχουν πιστοποιηθεί στο παρελθόν, και για τις οποίες έχει δημιουργηθεί και αποθηκευθεί ένα Κλειδί Σύνδεσης.

Άγνωστες συσκευές. Συσκευές για τις οποίες δεν υπάρχουν πληροφορίες ασφαλείας. Αντιμετωπίζονται ως μη πιστοποιημένες και ανάλογα με τις πληροφορίες που θα δεχτεί το σύστημα τις κατατάσσει στην κατηγορία των πιστοποιημένων ή μη συσκευών. (έμπιστες - μη έμπιστες).

Μη έμπιστες συσκευές. Συσκευές που δεν έχουν πιστοποιηθεί στο παρελθόν αλλά, έχει δημιουργηθεί και αποθηκευτεί ένα Κλειδί Σύνδεσης γι αυτές.

Έλεγχος πρόσβασης: Η πρόληψη μη εξουσιοδοτημένης χρήσης ενός πόρου, συμπεριλαμβανομένης της πρόληψης της χρήσης του πόρου με μη εξουσιοδοτημένο τρόπο.

Εμπιστευτικότητα: Η προστασία των επικοινωνιών ή των αποθηκευμένων δεδομένων από την υποκλοπή και την ανάγνωση από μη εξουσιοδοτημένα άτομα.

Εξουσιοδότηση: Η διαδικασία χορήγησης δικαιώματος πρόσβασης ή χρήσης μιας υπηρεσίας ή πληροφοριών, με βάση την έγκυρη ταυτότητα. Η εξουσιοδότηση χορηγείται από την οντότητα που ελέγχει τον πόρο για τον οποίο ζητείται η πρόσβαση.

Επίθεση: Οι δραστηριότητες που αποσκοπούν στην παράκαμψη ή την εκμετάλλευση των ατελειών των μηχανισμών ασφάλειας ενός συστήματος. Διακρίνονται σε άμεσες (εκμετάλλευση ατελειών αλγορίθμων, αρχών και ιδιοτήτων του μηχανισμού ασφάλειας) και έμμεσες επιθέσεις (υποχρέωση του συστήματος να χρησιμοποιήσει το μηχανισμό ασφάλειας με λανθασμένο τρόπο, παράκαμψη μηχανισμών).

Επικοινωνία: Κάθε είδους επικοινωνία μεταξύ ανθρώπων, αντικειμένων, ανθρώπων και αντικειμένων η οποία γίνεται είτε με τη μορφή του προφορικού ή γραπτού λόγου, είτε με τη μορφή μουσικής, ήχων και εικόνων, είτε με τη μορφή σημάτων είτε και με οποιοδήποτε συνδυασμό όλων αυτών των μορφών.

Θύρα επικοινωνίας: Ιδεατή θύρα επικοινωνίας μιας συσκευής που επιτρέπει τη διέλευση συγκεκριμένου τύπου πληροφορίας.

IEEE 802.11: Δέσμη πρωτοκόλλων που αφορούν τη λειτουργία ασύρματων τοπικών δικτύων, περιγράφοντας τα δύο πρώτα επίπεδα του OSI, δηλαδή το φυσικό επίπεδο και το επίπεδο σύνδεσης δεδομένων.

IEEE 802.1X: Πρωτόκολλο που επιτρέπει πιστοποίηση μέσω θυρών επικοινωνίας σε ασύρματα δίκτυα.

Κλειδί σύνδεσης: Το κλειδί σύνδεσης είναι ένας τυχαίος αριθμός. Ο χρόνος ζωής του εξαρτάται από το εάν είναι «ημιμόνιμο» ή «προσωρινό» κλειδί. Ένα προσωρινό κλειδί διαρκεί μόνο μέχρι να τερματιστεί η τρέχουσα σύνδεση και δεν μπορεί να ξαναχρησιμοποιηθεί στη συνέχεια.

Προστασία του απορρήτου: Η απαγόρευση της ακρόασης, της παγίδευσης, της αποθήκευσης, της επεξεργασίας, της ανακοίνωσης, της δημοσιοποίησης ή άλλου τύπου υποκλοπής ή παρακολούθησης της τηλεπικοινωνίας και των δεδομένων Επικοινωνίας από άλλα πρόσωπα, χωρίς την συγκατάθεσή τους, εξαιρουμένων των νόμιμα εξουσιοδοτημένων.

Πρωτόκολλο Εκτεταμένης Πιστοποίησης (EAP): Πρωτόκολλο που παρέχει τα απαραίτητα μηνύματα για εκτεταμένη πιστοποίηση μεταξύ τερματικής συσκευής και σημείου πρόσβασης.

Πρωτόκολλο ισοδύναμης ενσύρματης ιδιωτικότητας (WEP): Πρωτόκολλο που περιέχει τρεις διαδικασίες ασφάλειας, την κρυπτογράφηση των δεδομένων, την

προστασία της ακεραιότητας των δεδομένων και την πιστοποίηση της ταυτότητας του σταθμού.

Πρωτόκολλο RADIUS: Πρωτόκολλο που χρησιμοποιείται για την πιστοποίηση του χρήστη μέσω στοιχείων (όνομα και κωδικός πρόσβασης) σε ενσύρματα και ασύρματα δίκτυα.

Πρωτόκολλο DIAMETER: Βελτιωμένο πρωτόκολλο, σε σχέση με το RADIUS για την πιστοποίηση του χρήστη μέσω στοιχείων (όνομα και κωδικός πρόσβασης) σε ενσύρματα και ασύρματα δίκτυα.

Σταθερές τηλεπικοινωνιακές υπηρεσίες: Οι υπηρεσίες των οποίων η παροχή συνίσταται συνολικά ή εν μέρει στη μετάδοση και δρομολόγηση σημάτων μέσω σταθερών τηλεπικοινωνιακών δικτύων εξαιρουμένων των ραδιοφωνικών και τηλεοπτικών εκπομπών.

Συνδρομητής: κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών για την παροχή των υπηρεσιών αυτών.

Σταθερή ασύρματη πρόσβαση (ΣΑΠ): Ορίζεται από την ITU-R ως «ραδιοσυνδέσεις τελικών χρηστών με δίκτυα κορμού».

Σημεία πρόσβασης: Οι σταθεροί σταθμοί του δικτύου ασύρματων επικοινωνιών που χρησιμοποιούνται για την ασύρματη επικοινωνία με τα τερματικά του χρήστη.

Ταυτότητα: Οι πληροφορίες που προσδιορίζουν τον χρήστη τηλεπικοινωνιακής υπηρεσίας με μοναδικό τρόπο.

Τεχνολογία Bluetooth: Η τεχνολογία ασύρματης σύνδεσης δύο συσκευών, χωρίς να είναι απαραίτητη η οπτική επαφή μεταξύ τους.

Τηλεπικοινωνία: Η μεταφορά ήχων, σημάτων, εικόνων, δεδομένων, και εν γένει κάθε φύσης πληροφοριών μεταδιδόμενων εν όλω ή εν μέρει μέσω ενσύρματων, ασύρματων, ηλεκτρομαγνητικών, φωτοηλεκτρονικών ή φωτοοπτικών συστημάτων.

Τηλεπικοινωνιακός πάροχος: Φυσικό ή νομικό πρόσωπο που παρέχει τηλεπικοινωνιακές υπηρεσίες στο κοινό ή σε δημόσιο τηλεπικοινωνιακό δίκτυο. Όπου στο κείμενο αναφέρεται ο όρος χωρίς επεξήγηση θα εννοείται ο πάροχος τηλεπικοινωνιακών υπηρεσιών

Υπηρεσία κλήσης έκτακτης ανάγκης: Η υπηρεσία λήψης και διαχείρισης κλήσεων έκτακτης ανάγκης που γίνονται προς έναν τηλεφωνικό αριθμό και δρομολογούνται προς ειδικές κρατικές και μη Υπηρεσίες όπως είναι η Αστυνομία, η Πυροσβεστική Υπηρεσία, τα Νοσοκομεία κ.λπ.

Χρήστης: Κάθε φυσικό πρόσωπο ή νομική οντότητα που χρησιμοποιεί ή ζητά διαθέσιμη στο κοινό τηλεπικοινωνιακή υπηρεσία.

Χρήστης Παρόχου: Κάθε φυσικό πρόσωπο που ανήκει στο προσωπικό ή τους συνεργάτες του Παρόχου και χρησιμοποιεί τα συστήματα και τις υποδομές του Παρόχου.

ΚΕΦΑΛΑΙΟ ΙΙ
ΠΟΛΙΤΙΚΗ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΑΣΥΡΜΑΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 3
Ορισμός - Γενικές Απαιτήσεις και Συστάσεις

1. Πολιτική Διασφάλισης του Απορρήτου των Ασύρματων Τηλεπικοινωνιακών Υπηρεσιών (ΠΔΑΑΤΥ), είναι το σύνολο των κριτηρίων και κανόνων που καθορίζουν τις απαιτήσεις, τις υποχρεώσεις και τα δικαιώματα που διέπουν τη λειτουργία των τηλεπικοινωνιακών παρόχων και των χρηστών των τηλεπικοινωνιακών υπηρεσιών, με σκοπό την προστασία του απορρήτου της τηλεπικοινωνίας μέσω ασυρμάτων δικτύων επικοινωνιών.

2. Η ΠΔΑΑΤΥ θα εκπονείται από τους τηλεπικοινωνιακούς παρόχους διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών μέσω ασυρμάτων δικτύων με βάση τις απαιτήσεις και τις υποδείξεις του παρόντος Κανονισμού και θα εφαρμόζεται από αυτούς μετά την έγκρισή της από την ΑΔΑΕ.

3. Η ΠΔΑΑΤΥ αποτελείται από επί μέρους πολιτικές όπως είναι η Πολιτική Προστασίας των Δικτύων Ασύρματων Επικοινωνιών, η Πολιτική Επεξεργασίας δεδομένων Επικοινωνίας, η Πολιτική σε σχέση με το Προσωπικό και τους Συνεργάτες των Τηλεπικοινωνιακών Παρόχων, η Πολιτική Πρόσβασης, η Πολιτική Αποδεκτής Χρήσης και η Πολιτική Άρσης του Απορρήτου από τις οποίες απορρέουν τα δικαιώματα και οι υποχρεώσεις των εμπλεκομένων στη λειτουργία, τη διαχείριση και τη χρήση των τηλεπικοινωνιακών υπηρεσιών.

4. Η ΠΔΑΑΤΥ για να θεωρείται επαρκής θα πρέπει να διαθέτει τουλάχιστον τα ακόλουθα χαρακτηριστικά:

α) Να υλοποιείται μέσω διαδικασιών διαχείρισης συστημάτων, δημοσιοποίησης οδηγιών αποδεκτής χρήσης ή άλλων αντίστοιχων κατάλληλων μεθόδων.

β) Οι διαδικασίες, οι οποίες σχετίζονται με την υλοποίηση της πολιτικής, πρέπει να περιλαμβάνουν τουλάχιστον τον προσδιορισμό ταυτότητας, την αυθεντικότητα, την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εμπιστευτικότητα, την ακεραιότητα, την προστασία του απορρήτου, και τον έλεγχο παραβίασης του απορρήτου.

γ) Να εφαρμόζεται μέσω εργαλείων ασφάλειας ή/και μέσω διαδικασιών ασφάλειας.

δ) Να καθορίζει τα όρια ευθύνης των χρηστών και των χρηστών παρόχου. Επιπλέον οι μηχανισμοί μεταβολής της πολιτικής διασφάλισης του απορρήτου πρέπει να είναι καλά ορισμένοι, περιλαμβάνοντας τη διαδικασία, τους εμπλεκόμενους, καθώς και τους υπεύθυνους προς έγκριση.

5. Επίσης, συνιστάται η ΠΔΑΑΤΥ:

α) Να είναι ανεξάρτητη, στο μέτρο που είναι δυνατόν από τεχνικής απόψεως, από συγκεκριμένο εξοπλισμό (υλικό, λογισμικό) και

β) Να βασίζεται σε μια ανοικτή αρχιτεκτονική ώστε να καθίσταται βιώσιμη μακροπρόθεσμα.

Άρθρο 4
Χάραξη και Στοιχεία Πολιτικής Διασφάλισης Απορρήτου Ασύρματων Τηλεπικοινωνιακών Υπηρεσιών

1. Ένας τηλεπικοινωνιακός πάροχος προκειμένου να χαράξει την πολιτική του μπορεί, χωρίς να υποχρεώνεται ή να περιορίζεται, να ακολουθήσει τα παρακάτω βήματα:

α) Να προσδιορίσει τις πληροφορίες που πρέπει να προστατευτούν.

β) Να προσδιορίσει τα ευάλωτα σημεία του τηλεπικοινωνιακού δικτύου.

γ) Να προσδιορίσει τους κινδύνους και τις απειλές για τα α), β).

δ) Να προσδιορίσει τα μέτρα διασφάλισης του απορρήτου στις Ασύρματες τηλεπικοινωνιακές υπηρεσίες.

ε) Να καθορίσει τις υποχρεώσεις των υπαλλήλων και συνεργατών του.

στ) Να καθορίσει τις δεσμεύσεις και υποχρεώσεις του έναντι των πελατών. και

ζ) Να καταρτίσει σχέδιο αναθεώρησης και βελτίωσης της ΠΔΑΑΤΥ κάθε φορά που θα εντοπίζεται νέος κίνδυνος

ή αδυναμία ή που θα προκύπτουν νέες τεχνολογικές διευκολύνσεις διαχείρισης ασφάλειας.

2. Κάθε τηλεπικοινωνιακός πάροχος πρέπει, εν ανάγκη σε συνεργασία με τους παρόχους τηλεπικοινωνιακού δικτύου, να τεκμηριώνει με σχέδια την προστασία του απορρήτου για να αντιμετωπίζει προβλήματα που πιθανώς να εμφανισθούν σε έκτακτες περιστάσεις, όπως είναι η άρση του απορρήτου μετά από εντολή δικαστικών ή εισαγγελικών αρχών (Νόμος 2225/1994) και η προβληματική λειτουργία των τηλεπικοινωνιακών ή/και των μηχανογραφικών συστημάτων του ή των συστημάτων των συνεργατών του.

Άρθρο 5
Πληροφορίες που πρέπει να προστατεύονται

1. Κάθε πάροχος τηλεπικοινωνιακών υπηρεσιών μέσω ασυρμάτων δικτύων οφείλει να διασφαλίζει και να προστατεύει το απόρρητο των διαφόρων δεδομένων Επικοινωνίας, του περιεχόμενου της επικοινωνίας και εν γένει κάθε πληροφορίας που αφορά τους συνδρομητές του και χρησιμοποιείται για την παροχή της τηλεπικοινωνιακής υπηρεσίας, τη διεκπεραίωση της επικοινωνίας, κ.τ.λ.

2. Σε συγκεκριμένο φυσικό ή νομικό πρόσωπο, που είναι συνδρομητής ενός παρόχου ασύρματων τηλεπικοινωνιακών υπηρεσιών, πρέπει να προστατεύονται τα ακόλουθα στοιχεία εισερχομένων και απερχομένων κλήσεων.

α) Χρόνος και διάρκεια επικοινωνίας,

β) Εντοπισμός καλούντος ή και καλούμενου χρήστη,

γ) Στοιχεία που αφορούν στη χρέωση της επικοινωνίας,

δ) Περιεχόμενο επικοινωνίας,

ε) Ταυτότητα τερματικής συσκευής.

3. Οι πάροχοι ασύρματων τηλεπικοινωνιακών υπηρεσιών θα πρέπει να προσδιορίζουν τους κινδύνους και τις ενδεχόμενες απειλές για τα παραπάνω στοιχεία. Ο πάροχος οφείλει να διασφαλίζει την ασφαλή μετάδοση και αποθήκευση των δεδομένων επικοινωνίας που χρησιμοποιούνται σε ένα δίκτυο ασυρμάτων επικοινωνιών. Οι τηλεπικοινωνιακοί πάροχοι, όπου είναι απαραίτητο, από κοινού με άλλους παρόχους, εξασφαλίζουν ένα επίπεδο ασφάλειας που είναι ικανοποιητικό όσον αφορά την τεχνική ανάπτυξη και λογικό ως προς το κόστος του. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να ενημερώνει τους συνδρομητές του με συγκεκριμένους τρόπους και μέσα της επιλογής του για οποιουσδήποτε ειδικούς κινδύνους σχετικά με την ασφάλεια των υπηρεσιών που παρέχει καθώς και των δυνατοτήτων για την αποτροπή των κινδύνων και του κόστους των μέτρων που συνεπάγονται.

Άρθρο 6
Ευάλωτα Σημεία Δικτύου Ασυρμάτων Επικοινωνιών

1. Ευάλωτα σημεία τερματικών συσκευών χρηστών:

α) Η ίδια η συσκευή,

β) Τα ηλεκτρονικά τους αρχεία των εξερχόμενων ή εισερχόμενων κλήσεων,

γ) Το αρχείο των καλούντων και καλούμενων αριθμών,

δ) Ο τυχόν ενσωματωμένος αυτόματος τηλεφωνητής,

ε) Τυχόν μνήμη καταγραφής,

στ) Κάρτα Ταυτότητας Συνδρομητή.

2. Ευάλωτα σημεία δικτύου:

α) Σημεία πρόσβασης,

β) Ραδιοζεύξεις (μεταξύ σημείων πρόσβασης και τερματικών συσκευών),

γ) Αλγόριθμοι κρυπτογράφησης,

δ) Διακομιστές (servers),

ς) Κεντρικοί κατανεμητές παρόχου,

ζ) Σημεία διασύνδεσης και μεταγωγής του δικτύου ασύρματων επικοινωνιών με το σταθερό τηλεπικοινωνιακό δίκτυο,

η) Οι δρομολογητές κλήσεων όταν υπάρχει εκτροπή των κλήσεων σε εναλλακτικό φορέα παροχής τηλεπικοινωνιακών υπηρεσιών,

θ) Η αποκάλυψη κλειδιών που χρησιμοποιούνται για κρυπτογράφηση, ανασφαλές σύστημα χρέωσης ή δολιοφθορά.

3. Ο τηλεπικοινωνιακός πάροχος ασυρμάτων τηλεπικοινωνιακών υπηρεσιών θα πρέπει να ενημερώνει τους χρήστες για τα ευάλωτα σημεία των τερματικών συσκευών και να λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία εκείνων που υπάγονται στην περιοχή ευθύνης του.

ΚΕΦΑΛΑΙΟ III
ΕΠΙ ΜΕΡΟΥΣ ΠΟΛΙΤΙΚΕΣ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΑΣΥΡΜΑΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 7
Ασφάλεια Δικτύων Ασυρμάτων Επικοινωνιών Τεχνολογίας Bluetooth

1. Υπάρχουν τέσσερα είδη υπηρεσιών σε ότι αφορά την ασφάλεια των ασυρμάτων δικτύων τεχνολογίας Bluetooth: α) Υπηρεσίες που απαιτούν εξουσιοδότηση και πιστοποίηση της ταυτότητας. Αυτόματη πρόσβαση παρέχεται μόνο στις πιστοποιημένες συσκευές, ενώ οι υπόλοιπες θα πρέπει πρώτα να εξουσιοδοτηθούν. Η διαδικασία της εξουσιοδότησης πάντα εμπεριέχει την διαδικασία της πιστοποίησης της ταυτότητας, ώστε να διαπιστωθεί αν η απομακρυσμένη συσκευή είναι αυτή που ισχυρίζεται ότι είναι. β) Υπηρεσίες που απαιτούν την πιστοποίηση της ταυτότητας. Πριν αποκτήσει μια συσκευή πρόσβαση στην υπηρεσία θα πρέπει να πιστοποιήσει την ταυτότητά της. γ) Υπηρεσίες που απαιτούν κρυπτογράφηση των δεδομένων. Η σύνδεση θα πρέπει να μεταβεί στην κατάσταση κρυπτογράφησης των δεδομένων πριν εγκριθεί η πρόσβαση σε αυτές τις υπηρεσίες. δ) υπηρεσίες που είναι ανοικτές στις συσκευές. Για την πρόσβαση στις υπηρεσίες αυτές δεν απαιτείται καμιά διαδικασία ασφάλεια προηγουμένως.

2. Στην τεχνολογία Bluetooth πιστοποιείται η ταυτότητα της συσκευής και όχι του χρήστη.

3. Όλες οι διαδικασίες ασφαλείας στην τεχνολογία Bluetooth πραγματοποιούνται από το τμήμα που ονομάζεται διαχειριστής ασφάλειας. Ουσιαστικά ο διαχειριστής ασφάλειας αποφασίζει με βάση τα διάφορα δεδομένα που λαμβάνει ποια πολιτική ασφάλειας θα εφαρμόσει στην επικείμενη σύνδεση. Οι βασικές του λειτουργίες είναι: α) αποθήκευση πληροφοριών σχετικά με την ασφάλεια για όλες τις υπηρεσίες (Βάση Δεδομένων Υπηρεσιών), β) αποθήκευση πληροφοριών σχετικά με την ασφάλεια για τις γνωστές συσκευές (Βάση Δεδομένων Συσκευών) γ) απάντηση στις αιτήσεις για πρόσβαση από τις υλοποιήσεις των πρωτοκόλλων και τις εφαρμογές (παρέχει ή όχι πρόσβαση), δ) εφαρμογή της πιστοποίησης της ταυτότητας και/ή της κρυπτογράφησης των δεδομένων πριν συνδεθεί με την εκάστοτε εφαρμογή, ε) επεξεργασία δεδομένων από μια Εξωτερική Οντότητα Ελέγχου Ασφάλειας, για παράδειγμα από τον χρήστη της συσκευής, για να εγκαθιδρύσει έμπιστες σχέσεις στο επίπεδο της συσκευής και στ) ενεργοποίηση της διαδικασίας αρχικοποίησης μεταξύ δύο συσκευών και της εισαγωγής του Προσωπικού Αριθμού Αναγνώρισης από τον χρήστη. Εναλλακτικά η εισαγωγή του Αριθμού Αναγνώρισης μπορεί να γίνει και από την εφαρμογή που χρησιμοποιείται.

4. Περιπτώσεις απειλών του συστήματος ασφάλειας ενός ασύρματου δικτύου επικοινωνιών τεχνολογίας Bluetooth:
α) Επιθέσεις στη γεννήτρια τυχαίων αριθμών.
β) Επιθέσεις στον διαχειριστή ασφαλείας.
γ) Επίθεση στο αλγόριθμο E0.
δ) Επίθεση στο αλγόριθμο E1.
ε) Εντοπισμός θέσης του χρήστη στην ερευνητική κατάσταση λειτουργίας.
στ) Παρακολούθηση της συχνότητας λειτουργίας της συσκευής.

Άρθρο 8
Ασφάλεια Δικτύων Ασύρματων Επικοινωνιών IEEE 802.11

1. Σε ένα ασύρματο δίκτυο IEEE 802.11 πιστοποιείται μόνο η ταυτότητα του σταθμού και όχι η ταυτότητα του χρήστη. Πρέπει να έχει δύο συστήματα πιστοποίησης της ταυτότητας του σταθμού: το ανοικτό σύστημα πιστοποίησης, το οποίο αποτελεί την προεπιλεγμένη κατάσταση για την διαδικασία πιστοποίησης και στην ουσία δεν παρέχει πιστοποίηση, και το σύστημα κοινού κλειδιού, το οποίο χρησιμοποιεί το κοινό κλειδί για να πιστοποιήσει την ταυτότητα ενός σταθμού.
2. Σε ένα ασύρματο δίκτυο IEEE 802.11 με τη χρήση του πιστοποιητικού υπηρεσιών συσχετίζονται ένα ή περισσότερα σημεία πρόσβασης και με τη διαίρεση ενός ασύρματου δικτύου σε μικρότερα. Κάθε σημείο πρόσβασης μπορεί να προγραμματιστεί να δέχεται συγκεκριμένα πιστοποιητικά ώστε να υπάρχει πρόσβαση σε ορισμένα τμήματα του δικτύου. Με τον τρόπο αυτό μπορεί να περιοριστεί η πρόσβαση κάποιου σταθμού ή κάποιου χρήστη μόνο στα τμήματα του δικτύου που του είναι απαραίτητα. Το πιστοποιητικό υπηρεσιών λειτουργεί ισοδύναμα ως κωδικός πρόσβασης.
3. Συνοπτικά, για την ασφαλή διεξαγωγή της πιστοποίησης:
α) Επιβάλλεται τουλάχιστο η χρήση του WEP ως τεχνολογία πιστοποίησης στα ασύρματα δίκτυα IEEE 802.11.
β) Δεδομένων των μειονεκτημάτων του WEP και της πλειονότητας των δικτυακών συσκευών που υποστηρίζουν σήμερα EAP / IEEE 802.1X, συνιστάται η χρήση του συνδυασμού των πρωτοκόλλων IEEE 802.1X και EAP ως τεχνολογία πιστοποίησης στα ασύρματα δίκτυα IEEE 802.11.
4. Για λόγους ασφαλείας γενικώς έχουν αναπτυχθεί τεχνολογίες, οι οποίες βοηθούν τους χρήστες του δικτύου αφενός να αυξήσουν την ασφάλεια των συνδέσεων που πραγματοποιούν με χρήση του δικτύου και αφετέρου να διατηρήσουν το δικαίωμα της ανωνυμίας των διακινούμενων πληροφοριών που τους αφορούν. Οι μεν πρώτες είναι γνωστές ως τεχνολογίες ασφάλειας πληροφοριών (Information Security Technologies), οι δε δεύτερες ως τεχνολογίες αύξησης απορρήτου (Privacy Enhancing Technologies).
5. Πέρα από τις απαιτήσεις για ασφαλή πιστοποίηση, συνιστάται εφαρμογή αλγορίθμων ελέγχου ακεραιότητας και κρυπτογράφησης δεδομένων. Οι αλγόριθμοι MD5 και RC4 είναι οι πιο δημοφιλείς αλγόριθμοι στην κατηγορία αυτή και εγγυώνται ένα ικανοποιητικό επίπεδο ακεραιότητας και εμπιστευτικότητας της πληροφορίας.
7. Περιπτώσεις απειλών του συστήματος ασφαλείας ενός ασυρμάτου δικτύου της οικογένειας IEEE 802.11:
α) Επιθέσεις στα πιστοποιητικά υπηρεσιών.
β) Επιθέσεις στο πρωτόκολλο (WEP).
γ) Επιθέσεις στον αλγόριθμο RC4 του WEP.
δ) Επιθέσεις στους αλγορίθμους κρυπτογράφησης δεδομένων RC4 και MD5.
ε) Επιθέσεις στους αλγόριθμους κυκλικού ελέγχου και ελέγχου πλεονασμού.
στ) Επιθέσεις στα πρωτόκολλα EAP / 802.1X.
ε) Επιθέσεις στα ασύρματα ιδεατά ιδιωτικά δίκτυα (VPN).

Άρθρο 9
Ασφάλεια Δικτύων Σταθερής Ασύρματης Πρόσβασης και Δορυφορικών Δικτύων VSAT Επικοινωνιών

1. Τα δορυφορικά Δίκτυα VSAT ή τα δίκτυα σταθερής ασύρματης πρόσβασης (ΣΑΠ) είναι τεχνολογίες πρόσβασης και παροχής τηλεπικοινωνιακών υπηρεσιών υψηλών χωρητικοτήτων και ρυθμών. Οι σημαντικότερες υπηρεσίες είναι τηλεφωνία, μετάδοση δεδομένων, υπηρεσίες διαδικτύου μετάδοση video και τηλεδιασκέψεις (teleconferencing). Ένα δίκτυο VSAT αποτελείται κυρίως από έναν επίγειο δορυφορικό σταθμό υποδομής και έναν αριθμό τερματικών με συγκεκριμένη συνδεσμολογία. Οι σταθμοί VSAT ενδέχεται να είναι μεμονωμένοι ή να αποτελούν μέρος σε ένα ολοκληρωμένο δορυφορικό δίκτυο. Ένα δίκτυο ΣΑΠ είναι συνήθως κυψελωτό, και η κυψέλη χωρίζεται σε 4 τεταρτημόρια, όπου υπάρχει ένας σταθμός βάσης, ο οποίος επικοινωνεί με τους σταθερούς χρήστες LMDS.
2. Οι χρήστες τηλεπικοινωνιακών υπηρεσιών μέσω δικτύου VSAT ή ΣΑΠ έχουν τα παρακάτω δικαιώματα: α) Το δικαίωμα στην ασφάλεια και το απόρρητο των επικοινωνιών, β) Το δικαίωμα για τη λήψη ή όχι αναλυτικών λογαριασμών, γ) Το δικαίωμα στη μη αναγνώριση εισερχόμενης κλήσης, δ) Το δικαίωμα στην ενημέρωση για τα δεδομένα, ε) Το γενικό δικαίωμα αντίρρησης σε περαιτέρω χρήση των δεδομένων.
3. Η ΑΔΑΕ ελέγχει αν αυτά τα δικαιώματα παραβιάζονται από τους παρόχους των Ασύρματων Τηλεπικοινωνιακών Υπηρεσιών μέσω Δορυφορικών δικτύων VSAT και ΣΑΠ. Οι τηλεπικοινωνιακοί πάροχοι πρέπει να έχουν πάρει Ειδική Άδεια από την ΕΕΤΤ (όσων αφορά τη λειτουργία συγκεκριμένων ραδιοσυχνοτήτων) και Γενική Άδεια (για την παροχή όλων των υπολοίπων υπηρεσιών). Αν οι πάροχοι δορυφορικών υπηρεσιών είναι από άλλη χώρα, πρέπει να είναι έχουν νόμιμο αντιπρόσωπο στην Ελλάδα και να διαθέτουν ακριβώς τις ίδιες άδειες. Και στις δύο περιπτώσεις η ΑΔΑΕ θα διενεργεί ελέγχους σε εγκαταστάσεις και τεχνικό εξοπλισμό χρηστών και δορυφορικών παρόχων.

Άρθρο 10
Προστασία Δικτύων Ασυρμάτων Επικοινωνιών

1. Η ασφάλεια δικτύων ασυρμάτων επικοινωνιών περιλαμβάνει: α) τις απειλές που οφείλονται στην εμπεριεχόμενη αξιοπιστία του ίδιου του δικτύου ασυρμάτων επικοινωνιών και β) την ευαισθησία του στις απειλές από κακόβουλες πράξεις. Η απειλή μπορεί να προέλθει και από άλλο διασυνδεόμενο δίκτυο τηλεπικοινωνιών (σταθερών, κινητών) στο δίκτυο ασύρματων επικοινωνιών για το λόγο ότι η σηματοδοσία στο σταθερό τηλεφωνικό δίκτυο δεν είναι κρυπτογραφημένη. Η πολιτική ασφάλειας των παρόχων πρέπει να επιδιώκει να εντοπίζει τα σημεία που πρέπει να δοθεί ιδιαίτερη προσοχή.
2. Ο πάροχος οφείλει να λαμβάνει τα απαραίτητα μέτρα για την ασφαλή χωροθέτηση του τηλεπικοινωνιακού εξοπλισμού του, την προστασία των γραμμών μεταφοράς καθώς και όλων των δικτυακών στοιχείων, συμπεριλαμβα-

νομένων των κεραιών, ώστε να εξασφαλίζονται έναντι κακόβουλων επιθέσεων και έναντι άλλων μορφών φυσικών παρεμβάσεων.

3.Τα σημεία εισόδου από άλλα τηλεπικοινωνιακά δίκτυα πρέπει να ελέγχονται και ο αριθμός τους να είναι ο ενδεδειγμένος.

4. Πρέπει να λαμβάνονται όλα τα απαραίτητα μέτρα προστασίας για τα ευάλωτα σημεία του δικτύου που αναφέρονται στο άρθρο 7 του παρόντος.

Άρθρο 11
Προστασία Επεξεργασίας των Δεδομένων Επικοινωνίας

Οι τηλεπικοινωνιακοί πάροχοι ασυρμάτων τηλεπικοινωνιακών υπηρεσιών οφείλουν να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της κείμενης νομοθεσίας για την προστασία της επεξεργασίας των δεδομένων Επικοινωνίας.

Άρθρο 12
Ασφάλεια σε σχέση με τους Χρήστες Παρόχου

1. Οι χρήστες παρόχου οφείλουν να συμμορφώνονται με τις διατάξεις της νομοθεσίας περί προστασίας του απορρήτου και ειδικότερα:

α) Απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία που συνδέονται με: i) τα περιεχόμενα ή τα στοιχεία της επικοινωνίας που πραγματοποιείται μέσω παρόχου υπηρεσιών επικοινωνιών ή ii) τις υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα άλλο πρόσωπο μέσω ενός παρόχου υπηρεσιών επικοινωνιών ή iii) τα δεδομένα επικοινωνίας και υποπίπτουν στην αντίληψη ή στην κατοχή του, ως αποτέλεσμα της φύσης της εργασίας του.

β) Οι χρήστες παρόχου που διαχειρίζονται κλήσεις έκτακτης ανάγκης απαγορεύεται να αποκαλύπτουν πληροφορίες ή οποιαδήποτε στοιχεία συνδέονται με: i) τα περιεχόμενα ή την ουσία της επικοινωνίας που πραγματοποιείται μέσω του τηλεπικοινωνιακού παρόχου ή ii) τα δεδομένα Επικοινωνίας (όπως μη ανακοινώσιμες συνδέσεις και διευθύνσεις) που υποπίπτουν στην αντίληψη ή στην κατοχή τους, ως αποτέλεσμα της φύσης της εργασίας τους.

2. Οι εξαιρέσεις των προηγούμενων γενικών κανόνων θα πρέπει να περιγράφονται με σαφήνεια στην πολιτική ασφάλειας του τηλεπικοινωνιακού παρόχου.

Άρθρο 13
Πολιτική Πρόσβασης

1. Η Πολιτική Πρόσβασης καθορίζει το επίπεδο πρόσβασης χρηστών παρόχου και διεργασιών λογισμικού σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου για την παροχή των ασυρμάτων τηλεπικοινωνιακών υπηρεσιών.

2. Η Πολιτική Πρόσβασης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΑΤΥ.

3. Ο πάροχος οφείλει να διαθέτει και να εφαρμόζει πολιτική Πρόσβασης για τα συστήματα τα οποία αναφέρονται σε εξωτερικές συνδέσεις, επικοινωνίες φωνής και δεδομένων, τηλεπικοινωνιακές συσκευές και προγράμματα λογισμικού.

4. Η Πολιτική Πρόσβασης περιγράφει για κάθε σύστημα, με τρόπο λεπτομερή και σαφή, τουλάχιστον τις ακόλουθες διαδικασίες:

(α) Διαδικασίες προσθήκης νέων χρηστών και χρηστών παρόχου στο συγκεκριμένο δίκτυο ασυρμάτων επικοινωνιών.

(β) Διαδικασίες εξουσιοδότησης σχετικά με την προσθήκη, διαγραφή και αλλαγή των επιπέδων πρόσβασης των χρηστών παρόχου σε τηλεπικοινωνιακές υπηρεσίες του εν λόγω συστήματος.

(γ) Διαδικασίες ταυτοποίησης χρηστών.

(δ) Διαδικασίες ελέγχου των παραπάνω διαδικασιών και διαχείρισης του επιπέδου πρόσβασης που παραχωρείται στους χρήστες παρόχου.

(ε) Διαδικασίες πρόσβασης των χρηστών παρόχου των ασυρμάτων τηλεπικοινωνιακών υπηρεσιών σε συστήματα που διατηρούν δεδομένα κίνησης και θέσης χρηστών.

(στ) Σε περίπτωση που χρησιμοποιείται κρυπτογράφηση, η Πολιτική Πρόσβασης θα πρέπει να περιέχει τις διαδικασίες πρόσβασης των χρηστών παρόχου σε συστήματα κρυπτογράφησης/αποκρυπτογράφησης καθώς και σε διαδικασίες σχετικά με την διαχείριση, διανομή, εισαγωγή και αρχειοθέτηση των κλειδιών κρυπτογράφησης. Οι πληροφορίες αυτές θα αναφέρονται σε καταλλήλως διαβαθμισμένο παράρτημα των εγγράφων που περιέχουν την Πολιτική Πρόσβασης.

Άρθρο 14
Πολιτική Αποδεκτής Χρήσης

1. Η Πολιτική Αποδεκτής Χρήσης περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των χρηστών και χρηστών παρόχου των συστημάτων μετάδοσης του δικτύου ασυρμάτων επικοινωνιών ενός παρόχου.

2. Η Πολιτική Αποδεκτής Χρήσης αποτελεί αναπόσπαστο τμήμα της ΠΔΑΑΤΥ.

3. Σκοπός της είναι να διασφαλίσει ότι οι χρήστες και οι χρήστες παρόχου δεν θα εκμεταλλευτούν την πρόσβαση που τους παρέχεται σύμφωνα με την Πολιτική Πρόσβασης σε παντός είδους τηλεπικοινωνιακά δίκτυα προκειμένου να προβούν σε ενέργειες που παραβιάζουν οποιονδήποτε νόμο του κράτους ή σχετικό κανονισμό.

4. Η Πολιτική Αποδεκτής Χρήσης πρέπει να είναι προσαρμοσμένη στην κατηγορία χρηστών στην οποία απευθύνεται (χρηστών και χρηστών παρόχου) και να είναι σύμφωνη με την Πολιτική Πρόσβασης για κάθε κατηγορία χρηστών.

5. Η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει, με όσο το δυνατόν πιο λεπτομερή και κατανοητό τρόπο ώστε να αποφεύγονται οι παρερμηνείες, το ακόλουθο ελάχιστο περιεχόμενο:

(α) Δικαιώματα χρήστη και χρήστη παρόχου. Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης.

(β) Υποχρεώσεις χρήστη και χρήστη παρόχου. Σε αυτή την ενότητα περιλαμβάνονται μεταξύ άλλων συγκεκριμένα παραδείγματα μη αποδεκτής χρήσης των συστημάτων στα οποία ο χρήστης αποκτά πρόσβαση βάσει της Πολιτικής Πρόσβασης, καθώς και συνέπειες μη συμμόρφωσης με αυτές τις υποχρεώσεις.

(γ) Δικαιώματα του παρόχου τηλεπικοινωνιακών υπηρεσιών μέσω ασύρματων δικτύων.

(δ) Υποχρεώσεις του παρόχου τηλεπικοινωνιακών υπηρεσιών μέσω ασυρμάτων δικτύων.

6. Επιπλέον στην ενότητα που αναφέρεται στις υποχρεώσεις των χρηστών, η Πολιτική Αποδεκτής Χρήσης οφείλει να περιλαμβάνει τις παρακάτω διατάξεις οι οποίες σχετίζονται με την ασφάλεια του συστήματος:

(α) Οι χρήστες οφείλουν να λαμβάνουν όλα τα ενδει-

κνυόμενα μέτρα για την διασφάλιση του απορρήτου επικοινωνιών τους.

(β) Οι χρήστες οφείλουν να ενημερώνουν αμέσως τους υπευθύνους του παρόχου αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ιδίων ή άλλων χρηστών.

(γ) Οι χρήστες οφείλουν να αποκτούν πρόσβαση αποκλειστικά και μόνο σε δεδομένα κίνησης ή θέσης τα οποία αναφέρονται στους ίδιους ή είναι δημοσίως ανακοινώσιμα ή για τα οποία τους έχει δοθεί πρόσβαση από την Πολιτική Πρόσβασης.

(δ) Οι χρήστες απαγορεύεται να επιχειρούν να εκμεταλλευτούν πιθανά κενά ασφάλειας των συστημάτων του παρόχου προκειμένου να αποκτήσουν πρόσβαση σε πληροφορίες άλλων χρηστών, να διαταράξουν την ομαλή λειτουργία των δικτύων, να εκτελέσουν κακόβουλο λογισμικό και γενικά να υποβαθμίσουν το επίπεδο ασφάλειας του συστήματος.

7. Ειδικά σε σχέση με την ασφάλεια του τηλεπικοινωνιακού συστήματος, ο πάροχος οφείλει να συμμορφώνεται με τις διατάξεις του Κεφαλαίου III του παρόντος Κανονισμού.

8. Ο πάροχος οφείλει να δίνει στο χρήστη πρόσβαση στα συστήματά του μόνο εφόσον ο χρήστης έχει λάβει γνώση και ακολούθως έχει αποδεχθεί την Πολιτική Αποδεκτής Χρήσης. Το γεγονός αυτό αποδεικνύεται είτε με έγγραφη δήλωση του χρήστη η οποία φέρει την πρωτότυπη υπογραφή του ή εφόσον ο χρήστης έχει συμπληρώσει το αντίστοιχο πεδίο σε σχετική φόρμα αποδοχής στην περίπτωση που η Πολιτική Αποδεκτής Χρήσης παρουσιάζεται ηλεκτρονικά.

ΚΕΦΑΛΑΙΟ IV
ΥΠΟΧΡΕΩΣΕΙΣ ΦΟΡΕΩΝ, ΕΛΕΓΧΟΣ ΚΑΙ ΕΠΟΠΤΕΙΑ

Άρθρο 15
Υποχρεώσεις Παρόχων αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασυρμάτων Δικτύων

1. Όλοι οι τηλεπικοινωνιακοί πάροχοι υποχρεούνται:

(α) Να διαθέτουν ανά πάσα στιγμή καθορισμένη πολιτική για τη διασφάλιση του απορρήτου τηλεπικοινωνιακών υπηρεσιών παρεχομένων από δημόσια τηλεπικοινωνιακά δίκτυα ασύρματων επικοινωνιών.

(β) Να εφαρμόζουν την εν λόγω πολιτική.

(γ) Να ενημερώσουν σχετικά ως προς την εφαρμοζόμενη πολιτική την ΑΔΑΕ εντός έξι μηνών από την δημοσίευση του παρόντος.

(δ) Να εφαρμόζουν την εγκριθείσα από την ΑΔΑΕ πολιτική εντός ενός έτους από την έγκρισή της.

2. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβλέπει στο οργανόγραμμά του ξεχωριστή διοικητική οντότητα η οποία θα είναι επιφορτισμένη με την κατάρτιση και την εφαρμογή της ΠΔΑΑΤΥ με επικεφαλής κατάλληλα καταρτισμένο στέλεχός του που θα φέρει τον τίτλο του Υπευθύνου Ασφαλείας.

3. Για την αποτελεσματική εφαρμογή της Πολιτικής Πρόσβασης ο κάθε τηλεπικοινωνιακός πάροχος οφείλει να ορίζει τουλάχιστον:

(α) Έναν Υπεύθυνο Πρόσβασης, ο οποίος θα καθορίζει το είδος της πρόσβασης των χρηστών στα συστήματα.

(β) Έναν Υπεύθυνο Συστήματος, ο οποίος θα υλοποιεί τις αποφάσεις του Υπευθύνου Πρόσβασης.

(γ) Έναν Υπεύθυνο Αντιγράφων Ασφαλείας, ο οποίος πάντα σε συνεννόηση με τον Υπεύθυνο Πρόσβασης θα καθορίζει ποιός έχει πρόσβαση στα αντίγραφα ασφαλείας καθώς και κάθε πότε θα λαμβάνονται αντίγραφα ασφαλείας και για ποια δεδομένα.

4. Κάθε τηλεπικοινωνιακός πάροχος οφείλει να προβαίνει σε τακτικές επισκοπήσεις και αναθεωρήσεις της πολιτικής διασφάλισης του απορρήτου, είτε αυτόβουλα (μετά από έγκριση της ΑΔΑΕ σε περίπτωση αναθεώρησης) είτε ύστερα από σχετική εντολή της ΑΔΑΕ που μπορεί να προκύψει από πιθανή διαδικασία ελέγχου ή έκδοση σχετικής οδηγίας.

5. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου ο πάροχος οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους) και να παρέχει στοιχεία για την αποτροπή ή αντιμετώπισή τους.

6. Σε περίπτωση παραβίασης (ή ιδιαίτερου κινδύνου παραβίασης) της πολιτικής προστασίας του απορρήτου που δεν είναι δυνατό να αντιμετωπιστεί με τα τρέχοντα μέσα που διαθέτει ο τηλεπικοινωνιακό πάροχος, ο πάροχος οφείλει να ενημερώνει άμεσα τους συνδρομητές σχετικά με τους υφιστάμενους κινδύνους ασφάλειας και τις συνέπειες αυτών (συμπεριλαμβανομένου του πιθανού κόστους).

7. Ο πάροχος οφείλει να ορίζει συνέπειες για τη μη συμμόρφωση των χρηστών παρόχου με τα προβλεπόμενα από την ΠΔΑΑΤΥ (συμπεριλαμβανομένων των Πολιτικών Πρόσβασης και Αποδεκτής χρήσης).

Άρθρο 16
Διαδικασία Ελέγχου από την ΑΔΑΕ-Κυρώσεις

1. Η ΑΔΑΕ διενεργεί έκτακτους ελέγχους σε περίπτωση δημόσιων καταγγελιών ή έγγραφων καταγγελιών εκ μέρους των χρηστών. Εφόσον πρόκειται για δημόσιες καταγγελίες, ακολουθείται η διαδικασία που προβλέπεται για τους τακτικούς ελέγχους, ενώ στην περίπτωση εμπιστευτικών έγγραφων καταγγελιών εκ μέρους χρηστών, ο έλεγχος μπορεί κατά την κρίση της ΑΔΑΕ να γίνει αιφνιδιαστικά.

2. Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του παρόντος. Η συχνότητα των ελέγχων θα καθοριστεί από την ΑΔΑΕ με μεταγενέστερη Απόφασή της.

3. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες υπηρεσίες της ΑΔΑΕ ή από ειδικούς που τελούν υπό την άμεση επίβλεψη της ΑΔΑΕ με βάση τη διαδικασία που περιγράφεται στο Παράρτημα Α του παρόντος Κανονισμού.

4. Κατά την διάρκεια του ελέγχου η ΑΔΑΕ καταγράφει αναλυτικά τις ενέργειες σε ειδικό έντυπο με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Πάροχο Ασύρματων Τηλεπικοινωνιακών Υπηρεσιών αναφορικά με την Πολιτική Ασφάλειας και τη Διασφάλιση του Απορρήτου». Τα ελάχιστα απαραίτητα στοιχεία του εν λόγω εντύπου παρατίθενται στο Παράρτημα Β του παρόντος Κανονισμού.

5. Η ομάδα ελέγχου κοινοποιεί το πόρισμα της στην Ολομέλεια της ΑΔΑΕ. Η Ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου και είτε εγκρίνει τις ενέργειες που προβλέπονται στην εκάστοτε πολιτική ασφάλειας του παρόχου που έχει εγκριθεί από την ΑΔΑΕ είτε επιβάλλει κυρώσεις εφόσον δεν έχουν ληφθεί τα προσήκοντα μέτρα.

6. Ως προς τη διαδικασία και τις κυρώσεις της παραγράφου 1, ισχύουν οι διατάξεις του Νόμου 3115, άρθρο 11 και άρθρο 6, παράγραφος 4, καθώς και τα προβλεπόμενα στον εσωτερικό κανονισμό της ΑΔΑΕ (ΦΕΚ 1642/Β/7.11.2003).

Άρθρο 17
Άσκηση Εποπτείας

1. Κάθε πάροχος ασύρματων τηλεπικοινωνιακών υπηρεσιών στο τέλος του ημερολογιακού έτους υποχρεούται να υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν στην ασφάλεια των ασύρματων επικοινωνιών και τη διασφάλιση του απορρήτου.

2. Το ελάχιστο περιεχόμενο της ετήσιας έκθεσης ορίζεται ως εξής:

(α) Περιστατικά που απείλησαν την ασφάλεια του παρόχου και τη διασφάλιση του απορρήτου καθώς και τυχόν βλάβες που υπέστη ο πάροχος και οι χρήστες του εξαιτίας αυτών.

(β) Μέτρα που ελήφθησαν για την αντιμετώπιση των ως άνω περιστατικών.

3. Η ΑΔΑΕ με Απόφασή της δύναται να μεταβάλλει το ελάχιστο περιεχόμενο της ετήσιας έκθεσης.

Η ΑΔΑΕ δύναται να ζητήσει εκτάκτως από τους φορείς οποιεσδήποτε πληροφορίες θεωρεί αναγκαίες στα πλαίσια των αρμοδιοτήτων της για την ασφάλεια των ασύρματων επικοινωνιών και τη διασφάλιση του απορρήτου.

Άρθρο 18
Προστασία Επεξεργασίας Αρχείων

Σε περιπτώσεις παραβίασης των διατάξεων προστασίας του απορρήτου των επικοινωνιών, οι οποίες περιλαμβάνουν και επεξεργασία αρχείων που αφορούν την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η ΑΔΑΕ θα την ενημερώνει σχετικά προκειμένου να επιλαμβάνεται στο πλαίσιο των δικών της αρμοδιοτήτων.

ΚΕΦΑΛΑΙΟ V
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 19
Έναρξη Ισχύος

1. Ο παρών Κανονισμός τίθεται σε ισχύ από την ημερομηνία δημοσίευσής του στην Εφημερίδα της Κυβερνήσεως.

ΠΑΡΑΡΤΗΜΑ Α
Αναλυτική περιγραφή διαδικασίας Ελέγχου Τηλεπικοινωνιακού Παρόχου Ασύρματων Υπηρεσιών

Η διαδικασία ελέγχου παρόχου διενεργείται με βάση τα ακόλουθα βήματα:

(α) Η ΑΔΑΕ με Απόφασή της ορίζει ομάδα ελέγχου που αποτελείται από τρία (3) τουλάχιστον άτομα με σκοπό τον έλεγχο συγκεκριμένου παρόχου. Η ελαχίστη στελέχωση της ομάδας ελέγχου περιλαμβάνει έναν υπεύθυνο της ομάδας, έναν νομικό σύμβουλο και έναν τεχνικό σύμβουλο.

(β) Σε χρόνο που αποφασίζει η ομάδα ελέγχου, επικοινωνεί με τον πάροχο και ζητεί να έρθει σε άμεση επικοινωνία με τον υπεύθυνο ασφάλειας όπως αυτός ορίζεται στο κεφάλαιο IV του παρόντος. Τυχόν καθυστέρηση ή κώλυμα που παρουσιάζεται κατά την προσπάθεια επικοινωνίας με τον υπεύθυνο ασφάλειας καταγράφεται και φέρει τις ανάλογες κυρώσεις.

(γ) Ο υπεύθυνος ασφάλειας παραδίδει στην ομάδα ελέγχου πλήρες αντίγραφο της ΠΔΑΑΤΥ και των τυχών συνοδευτικών εγγράφων. Από τα παραδιδόμενα έγγραφα θα πρέπει να προκύπτουν οι ημερομηνίες έκδοσης και έγκρισης των συγκεκριμένων πολιτικών. Τυχόν καθυστέρηση επίδοσης σημειώνεται και φέρει τις ανάλογες κυρώσεις.

(δ) Η ομάδα ελέγχου προβαίνει σε αναλυτική εξέταση όλων των σχετικών εγγράφων ώστε να καταγραφούν οι τυχόν ελλείψεις που παρουσιάζονται στην πολιτική του παρόχου. Κατά τη διαδικασία αυτή δύναται να ζητηθεί η συνδρομή του παρόχου έτσι ώστε να διασαφηνιστούν τυχόν ασάφειες και προβλήματα που παρουσιάζονται στην πολιτική προστασίας του απορρήτου.

(ε) Κατά την διάρκεια του ελέγχου ο πάροχος δεν έχει την δυνατότητα να αντικαταστήσει την πολιτική προστασίας του απορρήτου με νέα ούτε να προβεί σε τυχόν διορθώσεις αυτής.

(στ) Σε περίπτωση ασαφειών ως προς την πολιτική προστασίας του απορρήτου οι πάροχοι, μετά από σχετική σύσταση της ΑΔΑΕ θα προβαίνουν στις απαραίτητες διορθώσεις στην πολιτική τους .

(ζ) Η ομάδα ελέγχου προβαίνει σε αυτοψία των εγκαταστάσεων του παρόχου για να διαπιστώσει σε ποιο βαθμό εφαρμόζονται οι διαδικασίες που προβλέπονται από τα προσκομιθέντα έγγραφα. Η αυτοψία δύναται να περιλαμβάνει και επαφή με το προσωπικό του παρόχου. Η ομάδα ελέγχου καταγράφει αναλυτικά τις ελλείψεις και τα σφάλματα που τυχόν διαπιστωθούν.

(η) Ο πάροχος οφείλει να υποβάλει στην ομάδα ελέγχου οποιοδήποτε στοιχείο θεωρηθεί απαραίτητο από την ομάδα για την επιτυχή ολοκλήρωση του ελέγχου.

(θ) Τυχόν διαπίστωση έλλειψης συνεργασίας από τον πάροχο ή/και προσπάθειας παραπλάνησης της ομάδας ελέγχου καταγράφεται και φέρει τις ανάλογες κυρώσεις.

ΠΑΡΑΡΤΗΜΑ Β
Ελάχιστο περιεχόμενο του εντύπου με τίτλο «Έκθεση Διενέργειας Ελέγχου σε Τηλεπικοινωνιακό Πάροχο αναφορικά με την Πολιτική Διασφάλισης του Απορρήτου των Ασύρματων Τηλεπικοινωνιακών Υπηρεσιών»

Το ως άνω έντυπο θα περιέχει απαραιτήτως τουλάχιστον τα ακόλουθα στοιχεία:

(α) Τα στοιχεία της Απόφασης της ΑΔΑΕ με την οποία αποφασίστηκε ο έλεγχος.

(β) Τα ονοματεπώνυμα και της ιδιότητες των στελεχών της ΑΔΑΕ που απαρτίζουν την ομάδα ελέγχου καθώς και την ημερομηνία σύστασής της.

(γ) Το όνομα του υπό έλεγχο παρόχου καθώς και το όνομα του υπευθύνου ασφάλειας του.

(δ) Το χρόνο που απαιτήθηκε έως ότου να παραδοθεί στην ομάδα ελέγχου η πλήρης πολιτική διασφάλισης απορρήτου του παρόχου.

(ε) Ημερολόγιο ενεργειών και ερωτήσεων της ομάδας ελέγχου και καταγραφή της ανταπόκρισης του ελεγχόμενου παρόχου.

(στ) Το αποτέλεσμα της αυτοψίας για την αποτίμηση της εφαρμογής της Πολιτικής Διασφάλισης της Προστασίας του Απορρήτου με καταγραφή τυχόν ελλείψεων και ασαφειών.

(ζ) Τις ημερομηνίες έναρξης και περάτωσης του ελέγχου.

(η) Τελικό πόρισμα του ελέγχου και εισήγηση προς την Ολομέλεια της ΑΔΑΕ.

Ο παρών Κανονισμός να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 12 Νοεμβρίου 2004

Ο Πρόεδρος
ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ

ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ